

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-129497

(43)Date of publication of application : 21.05.1996

(51)Int.Cl. G06F 11/30  
G06F 15/00  
H04M 11/00

(21)Application number : 06-269928

(71)Applicant : MITSUBISHI DENKI TOUBU  
COMPUTER SYST KK  
MITSUBISHI ELECTRIC CORP

(22)Date of filing : 02.11.1994

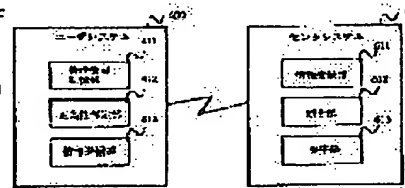
(72)Inventor : YANAGI SHOZO

## (54) MAINTENANCE SYSTEM, REMOTE MAINTENANCE METHOD AND REMOTE MAINTENANCE SYSTEM

### (57)Abstract:

PURPOSE: To simplify the collation of the opposite party when a line is connected and to reduce the time and expense by storing the control information of a user's system and checking the propriety.

CONSTITUTION: In the control information storage part 411 of the user's system 400, user's system information such as user's name and address, etc., and an H/W constitution and an S/W constitution, etc., is stored. Also, case body control information is simultaneously stored. These are checked by a propriety decision part 412 and the propriety of the system is judged. Further, an information transmission part 413 transmits user's system information to a center system 600 based on this decision result. In the the information registration part 611 of the center system 600, user's system information to be a maintenance object is preliminarily stored and the information is matched with received user's system information in a matching part 612. Based on the result, a maintenance part 613 starts maintenance. As a result, the protocol at the time of connecting a line is simplified and the information control of the user's system can be continuously performed without interposing input/out.



## LEGAL STATUS

[Date of request for examination] 08.02.1999

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-129497

(43) 公開日 平成8年(1996)5月21日

(51) Int.Cl. <sup>8</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 11/30	D	7313-5B		
15/00	3 3 0 A	9364-5L		
H 0 4 M 11/00	3 0 1			

審査請求 未請求 請求項の数10 O L (全 28 頁)

(21) 出願番号 特願平6-269928

(22) 出願日 平成6年(1994)11月2日

(71) 出願人 394013002

三菱電機東部コンピュータシステム株式会  
社

神奈川県横浜市戸塚区川上町87番地1

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 柳 昌三

横浜市戸塚区川上町87番地1 三菱電機東  
部コンピュータシステム株式会社横浜シス  
テムセンター内

(74) 代理人 弁理士 高田 守 (外4名)

(54) 【発明の名称】 保守システム及び遠隔保守方式及び遠隔保守システム

## (57) 【要約】

【目的】 情報管理を人手を介さず継続して行える保守システムを得る。また、障害通報時の解析情報の転送を選択的に行える遠隔保守システムを得る。

【構成】 ユーザシステムの管理情報記憶部にソフトウェアで読み出し可能な筐体管理情報を記憶させることにより、正当性判定部がユーザシステムの正当性を判定し、システム構成情報を情報送信部がセンタシステムに送信する。センタシステムの照合部が情報登録部と照合後、保守部が保守を開始する。

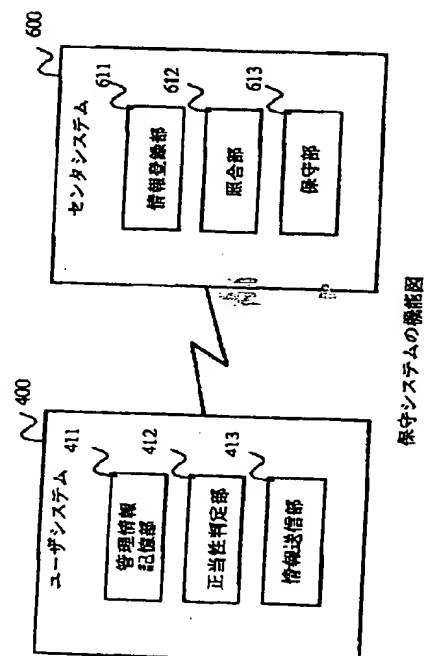


図1 保守システムの構成図

## 【特許請求の範囲】

【請求項1】 以下のユーザシステムとセンタシステムを備えた保守システム

(a) 以下の要素を備えたユーザシステム

(a 1) ユーザシステムの管理情報を記憶する管理情報記憶部、(a 2) 上記管理情報をチェックすることによりシステムの正当性を判定する正当性判定部、(a 3) 上記正当性判定部の判定結果に基づいて、センタシステムにユーザシステムの情報を送信する情報送信部、

(b) 以下の要素を備えたセンタシステム

(b 1) 保守の対象となるユーザシステムの情報を記憶する情報登録部、(b 2) 上記情報送信部により送信された情報を受信し、情報登録部に記憶された情報と照合する照合部、(b 3) 上記照合部の照合結果に基づいて、ユーザシステムの保守を開始する保守部。

【請求項2】 上記管理情報記憶部は、ユーザシステム本体の一部として存在し、システム構成の変更及びシステムを構成する部品の変更により変更されることがない筐体管理情報を記憶することを特徴とする請求項1記載の保守システム。

【請求項3】 上記情報送信部は、ユーザシステムのシステム構成情報を送信し、上記情報登録部は、受信したシステム構成情報を記憶し、上記保守部は記憶されたシステム構成情報を参照してユーザシステムの保守を実行することを特徴とする請求項1又は2記載の保守システム。

【請求項4】 障害通報に基づいて保守解析情報を収集して保守センタに転送する遠隔保守方式において、保守解析情報を基本情報と複数の補足情報に分割して収集する収集手段と、複数の補足情報の中から転送する補足情報を選択する選択手段と、基本情報と選択された補足情報を回線を用いて保守センタに転送する転送手段を備えたことを特徴とする遠隔保守方式。

【請求項5】 上記選択手段は、転送手段が使用する回線の種別に応じて転送する補足情報を選択することを特徴とする請求項4記載の遠隔保守方式。

【請求項6】 上記収集手段は、収集した補足情報の目録を作成し、上記転送手段は目録を保守センタに転送することを特徴とする請求項4又は5記載の遠隔保守方式。

【請求項7】 上記目録は、各補足情報に対応してその補足情報の存在場所を示す情報を有していることを特徴とする請求項6記載の遠隔保守方式。

【請求項8】 保守センタが回線を用いてユーザシステムを保守する遠隔保守システムにおいて、上記保守センタに、ユーザシステムに対して接続要求を出す接続要求手段と、

ユーザシステムからの接続応答に対して折り返し接続要求を出す折り返し接続要求手段と、回線の接続を切断する回線切断手段を備え、上記ユーザシステムに、

05 上記接続要求手段に基づく接続要求に対して応答する応答手段と、

上記折り返し接続要求手段に基づく折り返し接続要求に対して接続要求を出す折り返し手段を備えたことを特徴とする遠隔保守システム。

10 【請求項9】 保守センタが回線を用いてユーザシステムを保守する遠隔保守システムにおいて、上記保守センタに、

回線を接続してユーザシステムに対して作業指示を出す指示手段と、

15 指示手段による作業指示の作業時間を判定する判定手段と、

判定手段の判定結果に基づいて、回線の接続を切断する回線切断手段を備え、上記ユーザシステムに、

20 上記指示手段による指示を実行する実行手段と、実行手段による実行終了後、回線の接続状態をチェックする回線状態判定手段と、

回線状態判定手段の判定結果に基づいて、回線を接続する回線接続手段を備えたことを特徴とする遠隔保守システム。

25 【請求項10】 上記遠隔保守システムは、少なくとも保守センタとユーザシステムのいずれかに、回線費用負担情報を表示することを特徴とする請求項8又は9記載の遠隔保守システム。

30 【発明の詳細な説明】

【0001】

【産業上の利用分野】この発明は通信回路を介してユーザシステムの保守を行う遠隔保守システムに関するものである。

35 【0002】

【従来の技術】従来の遠隔保守システムにおける保守対象システムの情報管理は、遠隔保守システムの管理番号であるユーザ識別子を用いるか、あるいは、ユーザシステムのCPUシステム番号で行っている。また、回線接続時の保守対象（ユーザシステム）確認は、ユーザ識別子と接続時のパスワードや回線番号を利用したコールバック等により行っている。図32は、従来の保守対象確認時の手順を示す図である。図32(a)はパスワードによるユーザ照合の手順である。まず、ユーザシステムより接続要求を保守センタに送り出す。(1)

続いて、ユーザ識別子を保守センタに送る。(2)

次に、保守センタでは、送られたユーザ識別子を用いてユーザ管理情報を参照し、ユーザの照合を行う。(3)

次に、保守センタでは正当なユーザであることを照合するために、パスワードを要求する。(4)

そのパスワード要求に基づいて、ユーザシステムはパスワードを保守センタに送信する。(5)

保守センタでは送信されたパスワードをユーザ管理情報と照合する。(6)

正当なユーザであることを確認した後、保守サービスを開始する。(7)

以上がパスワードによるユーザ照合の手順である。また、図32(b)はコールバック方式による保守対象ユーザシステムの対象確認の手順である。まず、ユーザシステムは、保守センタに対して接続要求を送り出す。

(1)

保守センタでは、接続要求を受け取ると接続待ち指示を出す。(2)

ユーザシステムでは接続待ち指示を受けて、保守センタからのコールバック待ちになる。(3)

この間保守センタでは、ユーザ管理情報を参照してユーザ照合を行う。(4)

ユーザ管理情報よりユーザシステムの回線番号を用いて接続要求をユーザシステムに対して送り出す。(5)

この接続要求に対してユーザシステムが接続応答を返すと(6)、

保守センタでは保守サービスを開始する。(7)

すなわち、このコールバック方式においては、保守センタが管理しているユーザ管理情報に登録されている回線番号を用いて接続要求を出した場合に接続応答を返すことによって、正当なユーザであると見なされ、保守サービスを受けることができる。この方法では、保守対象のユーザシステムの確認はCPUシステム番号によって行われているが、CPUシステム番号は何らかの理由でCPU交換が発生した場合に変更されてしまう。また、回線番号によるコールバックは保守対象のユーザシステムが移転する場合に回線番号が変わってしまうという不都合があった。このような事象が発生すると、管理情報の整合性を保証するための人手による作業が発生するだけでなく、変更確認においてもコールバック等の確認を必要とするという問題点があった。

【0003】図33は従来の障害発生から保守センタによる修復までの手順を示す流れ図である。図にそって説明する。まず、ユーザシステムにおいて障害が発生すると、保守解析情報がセーブされる。その後、保守センタに対して障害発生が通報される。通報時には、まず、定型的な解析情報が保守センタに対して送信される。保守センタでは受信した解析情報を用いて一次解析を行い、さらに、一次解析の結果に基づいてより詳細な資料を採取する。採取した詳細資料を用いて分析を行い、修復方法をユーザシステムに対して指示する。ユーザシステムでは、指示された方法を用いて修復を行う。このような障害通報における保守解析情報は、保守センタにとって必要不可欠の情報であるが以下の理由により必要最低限の情報を抽出し、通報時に添付していた。

(1) 回線費用の軽減を図る。

(2) 障害通報時に停止する業務の再開を急ぐために短時間で通報を完了させる。

一方、ソフトウェア障害の様に多種多様な障害を扱う場合、一様に抽出された情報では根本的な原因追及には情報が不足し、遠隔保守で解析できる障害の範囲に制約が発生するという問題点があった。

【0004】また、通常、NTTの回線を利用する場合、回線契約時に回線費用の負担は発呼側か着呼側か一方に決定されてしまう。保守センタの様に多種多様な相手や多種多様なサービスを提供しなければならない場合、用途に応じて複数の回線を必要とすることがあった。きめ細かなサービスを提供するには1本の回線を多用途に利用できるようにする必要がある。

【0005】図34は、特開平3-85646号公報に開示された遠隔保守システムのブロック図である。図において、901は情報処理システム、902はサービスプロセッサ、903は機種タイプ保持手段、904及び905は通信制御手段、906は遠隔保守センタ、907は通信回線である。この従来例は情報処理システム901が機種タイプ保持手段903に機種情報を持ち、その機種情報を遠隔保守センタ906に渡すことによって機種に応じた保守制御が確実に受けられるという遠隔保守システムである。この従来例によれば、例えば、機種

の判別を誤って適切な遠隔保守サービスを受けられないという問題点は解決されている。ところが、機種タイプ保持手段903は機種毎の識別情報は持っているが、個々の情報処理システムに対してユニークな識別子を設けてはいない。すなわち、このシステムは、個々の情報処理システムを管理するというシステムではない。

【0006】図35は特開平5-14576号公報に開示されたファクシミリリモートサービスシステムを適用したファクシミリ装置のブロック図である。図において、911はファクシミリ装置、912はCPU、913はROM、914はRAM、915は操作部、916はスキャナ、917はプロッタ、918はDTMFレシーバ、919はNCU、920はモデム、921はバスである。この従来例はファクシミリリモートサービスシステムにおいてファクシミリ装置でリモートサービス用のIDコードを登録し、サービスセンタから同一のリモートサービスIDが入力された場合にのみファクシミリ装置内部のRAM914に記憶された情報、例えば、通信履歴情報や内部設定情報をサービスセンタに送信するという方式を取ることによって、ファクシミリ装置内の情報が他社に漏洩することを防止する目的を持つものである。従って、ファクシミリ装置毎にユニークなIDを用いるリモート保守システムではあるが、そのリモートサービスIDを用いて、サービスセンタからより付加価値の高い個別の保守情報を得ることを目的としたものではない。

【0007】図36は特開昭63-300328号公報に開示された遠隔保守方式のブロック図である。図において、912は中央処理装置、931はログ収集手段、932は自動通報判定手段、941はセンタ呼出し手段、942は通報送出手段である。また、961から969は周辺装置であり、それぞれ障害検出手段971から979を備えている。この従来例では周辺装置に障害が発生した場合、障害検出手段を用いて発生した障害を検出し、ログ収集手段が収集したログ情報を解析することによって、遠隔保守センタに対する障害通知を行うかどうかの判定を自動通報判定手段932が行うことを特徴としている。

【0008】図37は特開昭60-181940号公報に開示されたリモート保守方式のブロック図である。図において、953はフロッピーディスク、954はコンソール、955は保守試験制御部、956は操作制御部、957は転送制御部である。この従来例では保守に関する処理に伴ってやり取りされる一連の情報の内、予め指定されたものを選択してコンソールに出力する手段を設けたものである。これにより、解析に必要な情報のみが選択されるので、転送時間が短縮され、また、データの蓄積が効率的になるという長所を備えたものであるが、選択の基準は解析に必要な情報がどうかであり、使用する通信回線等は考慮されていない。

#### 【0009】

【発明が解決しようとする課題】この発明は上記のような問題点を解消するためになされたものであり、以下の各点を目的としている。

(1) 保守対象のユーザシステムの確認に筐体情報を用いることにより、接続時のプロトコルを簡略化する。さらに、ユーザ情報の管理においてユーザシステムの更新履歴の連続性を保つ。

(2) 保守センタへの解析情報を細分化し、選択可能とすることにより、多種多様な障害に対応できる遠隔保守方式を得る。

(3) 回線接続において、必要に応じて一時切断することが可能な遠隔保守システムを得る。また、ユーザシステムからの折り返し接続が可能な遠隔保守システムを得る。

#### 【0010】

【課題を解決するための手段】この発明の保守システムは以下のユーザシステムとセンタシステムを備えたことを特徴とする。

(a) 以下の要素を備えたユーザシステム

(a 1) ユーザシステムの管理情報を記憶する管理情報記憶部、(a 2) 上記管理情報をチェックすることによりシステムの正当性を判定する正当性判定部、(a 3) 上記正当性判定部の判定結果に基づいて、センタシステムにユーザシステムの情報を送信する情報送信部、

(b) 以下の要素を備えたセンタシステム

(b 1) 保守の対象となるユーザシステムの情報を記憶する情報登録部、(b 2) 上記情報送信部により送信された情報を受信し、情報登録部に記憶された情報と照合する照合部、(b 3) 上記照合部の照合結果に基づい

て、ユーザシステムの保守を開始する保守部。

【0011】上記管理情報記憶部は、ユーザシステム本体の一部として存在し、システム構成の変更及びシステムを構成する部品の変更により変更されることがない筐体管理情報を記憶することを特徴とする。

【0012】上記情報送信部は、ユーザシステムのシステム構成情報を送信し、上記情報登録部は、受信したシステム構成情報を記憶し、上記保守部は記憶されたシステム構成情報を参照してユーザシステムの保守を実行することを特徴とする。

【0013】また、この発明の遠隔保守方式は、保守解析情報を基本情報と複数の補足情報に分割して収集する収集手段と、複数の補足情報の中から転送する補足情報を選択する選択手段と、基本情報と選択された補足情報を回線を用いて保守センタに転送する転送手段を備えたことを特徴とする。

【0014】上記選択手段は、転送手段が使用する回線の種別に応じて転送する補足情報を選択することを特徴とする。

【0015】上記収集手段は、収集した補足情報の目録を作成し、上記転送手段は目録を保守センタに転送することを特徴とする。

【0016】上記目録は、各補足情報に対応してその補足情報の存在場所を示す情報を有していることを特徴とする。

【0017】この発明の遠隔保守システムは、上記保守センタに、ユーザシステムに対して接続要求を出す接続要求手段と、ユーザシステムからの接続応答に対して折り返し接続要求を出す折り返し接続要求手段と、回線の接続を切断する回線切断手段を備え、上記ユーザシステムに、上記接続要求手段に基づく接続要求に対して応答する応答手段と、上記折り返し接続要求手段に基づく折り返し接続要求に対して接続要求を出す折り返し手段を備えたことを特徴とする。

【0018】この発明の遠隔保守システムは、上記保守センタに、回線を接続してユーザシステムに対して作業指示を出す指示手段と、指示手段による作業指示の作業時間を判定する判定手段と、判定手段の判定結果に基づいて、回線の接続を切断する回線切断手段を備え、上記ユーザシステムに、上記指示手段による指示を実行する実行手段と、実行手段による実行終了後、回線の接続状態をチェックする回線状態判定手段と、回線状態判定手段の判定結果に基づいて、回線を接続する回線接続手段を備えたことを特徴とする。

【0019】上記遠隔保守システムは、少なくとも保守センタとユーザシステムのいずれかに、回線費用負担情

報を表示することを特徴とする。

【0020】

【作用】この発明の保守システムにおいては、ユーザシステムの管理情報記憶部が管理情報を記憶し、正当性判定部がこの管理情報をチェックすることにより、システムの正当性を判定する。さらに、判定結果に基づいて、センタシステムにユーザシステムの情報を情報送信部が送信する。センタシステムでは、情報登録部が、保守の対象となるユーザシステムの情報を記憶し、ユーザシステムの情報送信部より送信された情報を受信し、照合部が情報登録部に記憶された情報と照合する。その照合結果に基づいて、保守部がユーザシステムの保守を開始する。

【0021】管理情報記憶部は、ユーザシステム本体の一部として存在する筐体管理情報を記憶するので、システム構成の変更や部品の変更により変更されることがない。

【0022】情報送信部は、ユーザシステムのシステム構成情報を送信し、受信したシステム構成情報を情報登録部が記憶する。保守部は情報登録部に記憶されたシステム構成情報を参照してユーザシステムの保守を実行するので、確実に最新のユーザシステムのシステム構成にあった保守が行われる。

【0023】障害通報に基づいて保守解析情報を収集する際、収集手段は保守解析情報を基本情報と複数の補足情報に分割して収集し、選択手段は複数の補足情報の中から転送する補足情報を選択する。転送手段は基本情報と選択された補足情報を回線を用いて保守センタに転送するので、優先度の高い情報を転送することができる。

【0024】さらに、選択手段は、転送手段が使用する回線の種別に応じて、転送する補足情報を選択するので、効果的な選択が可能となる。

【0025】転送手段は、収集手段が作成した情報の目録を保守センタに転送するので、保守センタ側では、その目録を参照することによって補足情報に関する情報を得ることができる。

【0026】目録は、各補足情報に対応してその補足情報の存在場所を示す情報を有しているので、目録を参照することによって、全ての保守解析情報の存在場所を把握することが可能となる。

【0027】保守センタは、接続要求手段を用いてユーザシステムに対して接続要求を出し、その接続要求に対してユーザシステムの応答手段が応答する。保守センタでは、ユーザシステムからの接続応答に対して、折り返し接続要求手段が折り返し接続要求を出し、ユーザシステムでは、その折り返し接続要求に対して折り返し手段が接続要求を出す。一方、保守センタでは、折り返し接続要求を出した後、回線切断手段が回線の接続を切断する。

【0028】この発明の遠隔保守システムにおいては、

保守センタの指示手段が回線を接続してユーザシステムに対して作業指示を出し、判定手段がその作業指示の作業時間を判定し、判定結果に基づいて回線切断手段が回線の接続を決断する。一方、ユーザシステムでは、実行手段が指示手段による指示を実行する。また、実行終了時に、保守センタ側が回線を切断しているかどうか不明なため、回線状態判定手段が回線の接続状態をチェックする。チェックした結果、回線が接続されていないければ、回線接続手段が改めて回線を接続する。

【0029】この遠隔保守システムにおいては、保守センタとユーザシステムのいずれか、あるいは両方に回線費用負担情報を表示する。それにより、オペレータ、あるいは保守員は回線費用が発生しているかどうかを知ることができる。

【0030】

【実施例】

実施例 1. この実施例では、ユーザシステム側で、システム立ち上げ時に正当なシステムであることを毎回確認する保守システムについて説明する。まず、図 1 を用いて、この実施例の概略について説明する。この実施例では識別カードを用いて正当性を判定する。図 1 はこの実施例のブロック図である。1 は識別カード、2 は被プロテクトノードを記述した管理データテーブル、3 はセキュリティ管理プログラム、4 は被プロテクトノード、5 は計算機筐体に設けられた個別の識別子、6 は識別カードリーダー/ライター、7 は SVP (サービスプロセス)、8 は中央処理装置、9 は遠隔地計算機、10 は計算機本体、11 は公衆回線である。

【0031】識別カード 1 には被プロテクトノードを記述した管理データテーブル 2 とセキュリティ管理プログラム 3 が格納されている。管理データテーブル 2 には、被プロテクトノード 4 の使用可否、及び使用期限等のデータが入っている。被プロテクトノードとはオプションのハードウェア (以下 H/W)、及びソフトウェア (以下 S/W) である。また、識別カード 1 内には、データの不法読み取り、不法改ざん防止の為、セキュリティ管理プログラム 3 が用意されており、SVP 7 は管理データテーブルへのアクセスの際、識別カード 1 に固有の識別子を送らなければならない。識別カード 1 はその識別子の整合がとれた場合だけ管理データテーブルへのアクセスを許可する。セキュリティ管理プログラム 3 と SVP 7 は識別子認証を行い、セキュリティ管理プログラム 3 は指定された識別子を送ってきた計算機に対してのみ識別カード 1 の管理データテーブル 2 のアクセスを許可する。

【0032】識別カード 1 の個別の識別子は計算機筐体に設けられた個別の識別子 (たとえば、CPU システム番号あるいは筐体番号) 5 と同一のものであり計算機据え付け時の起動で一回のみ SVP 7 により識別カード 1 に書き込まれる。以降その個別の識別子がシステム立ち

上げごとに認証に使用される。

【0033】この動作を図2を用いて説明する。システムたち上げ時にシステムのコンフィグレーション或はイニシャルプログラムロードを行う際、筐体の識別子5、識別カードリーダ/ライタ6、被プロテクトノード4とインタフェースを持つSVP7は計算機筐体に設けられた個別の識別子5と識別カード1に格納された個別の識別子との認証をセキュリティ管理プログラム3を用いて行ない(S1)、整合がとれなければそこで、システムたち上げを中止する(S7)。

【0034】整合がとれた場合(S2)、システムのコンフィグレーション或はオペレーティングシステムのイニシャルプログラムロードを行うが、SVP7はその時の被プロテクトノード4の使用可否(S3)、使用期限(S4)を識別カード1の管理データテーブル2を通して知り、認証された内容に従って、インストレーション或はロードの行う(S5)。このチェックを管理データテーブル2に定義されたすべての被プロテクトノードについて行い(S6)、システムを立ち上げる。

【0035】次に図3を用いて、OS(オペレーティングシステム)41のもとで動くアプリケーションプログラム42a~42nが起動される場合のチェックについて説明する。SVP7を通して、識別カード1内の管理データテーブル2との照合がオペレーティングシステム内のユーザプログラムセキュリティ管理マネージャ41aによって行われ、許可されている場合はそのまま起動され、許可されていない場合は起動を中止される。また、SVP7は遠隔地との通信機能を持つ。遠隔地計算機9は、公衆回線11を通して遠隔地からの通信により、識別カード1へアクセスし、管理データテーブル2の更新を行う。

【0036】次に、この実施例の詳細について、以下に説明する。なお、以下においては、識別カード1が、ICカードであり、識別子を筐体番号として説明する。さらに、前述したユーザプログラムセキュリティ管理マネージャ41aをSVC(スーパーバイザーコール)インタフェースのチェックシステムコールで起動できるルーチンとして説明する。

【0037】まず、システムの概要について述べる。・CPUシステム番号(筐体番号)と対になったICカードがあり、正規のICカードがセットされなければシステムは基本的には立ち上がらない。・OSがICカードに格納されている管理データテーブルを読み出し、その内容に従って被プロテクトノードとして記憶された資源の機能をユーザに使用させるかどうか制御する。

【0038】これらは、S/Wの不正使用を防止する目的で行うが、6)は他システムからのモジュールの不正なコピー防止を目的とするものである。このシステムでは、すべてのメーカ標準S/Wが、MT(マグネティックテープ)あるいは、DAT(デジタルオーディオテー

プ)に格納された状態で客先へ出荷される。客先では、その内容物すべてを、OS専用領域を持つディスクヘインストールする。OS専用領域は、MT内あるいはDAT内のS/W類、スワップ/ダンプ領域、および、各S/W独自に必要なとするディレクトリを含み、将来性を考えた十分な大きさを持ち、大きさは固定とする。このOS専用領域には、ユーザのプログラムやデータの格納を禁止する。

【0039】次に、ICカードのメモリ構造、および、メモリに書き込まれる情報について述べる。

【メモリ構造】メモリにはフラッシュメモリ(またはEPROM等でもよい)が使用され、図4に示すようにシステム領域とユーザ領域の2つに大別される。

【0040】【ICカードに書き込むデータ】システム領域には、ICカード自身の管理情報とユーザ管理情報が書き込まれる。

(1) PIN(Personal Identification Number)

PINは、利用者確認番号であり、この実施例では、システム設置後最初のIPL時にPINに筐体番号を設定し、次回以降のIPL時にPINを照合する。設定されたPINとICカードが装着されたマシンの筐体番号を照合することにより、1つのICカード内の情報(契約した資源を供給する情報)が特定のマシン以外では使用できないようにする。照合の結果が正しい場合には、ユーザ領域に設けられたADF(Application Data File)の内容に従って資源単体毎に動作可否が決定され、不正の場合には縮退モードでのシステム稼働となる。

(2) ICカード識別情報

ICカード識別情報とは、ICカードのH/W情報(メモリの種類や容量、ICカード自身のバージョン、ICカードのシリアル番号等)が書き込まれている。

(3) ユーザ管理情報

ユーザ(使用者)についての情報を管理するための領域であり、ICカード発行の際にユーザ情報が営業部門のユーザ管理D/B(顧客管理データベースとも呼ぶ)をもとに書き込まれる。

(4) ADF(Application Data File)

ADFはICカードのユーザ領域をアクセスする際の1つの単位で、ユーザ領域を使用するためには、初めにADFを作成(指定されたADF-IDに対応する領域をユーザ領域に確保)しなければならない。ADFを作成する際には、APW(ADF毎のパスワード)とアクセス・レベルの指定が必要となる。

【0041】ユーザ領域では、ADF毎に分けて、メーカ側はADFの使用領域の管理とOSの核(カーネル)のもとで動くS/W(メーカ基本S/W)の管理を行い、販社では販社毎に決められた情報を管理する。以



下、各管理情報毎に述べる。

(1) ADF毎の使用領域管理情報：各ADF毎の総バイト数と使用バイト数、空きバイト数の管理を行う。

(2) S/W管理情報：S/Wの管理を行い、S/W別の版名、使用開始日、有効期限、使用可否、製品クラス番号等の情報を管理する。

例えば、ソフトウェア毎の識別IDはソフトウェアの種類毎に固有であり、同じソフトウェアであれば共通の識別子である。プロダクトコード、S/W名も同様である。一方、クラス、有効期限開始日、有効期限終了日等はユーザ固有の情報であり、そのユーザの契約内容を反映させた情報が書き込まれる。

【0042】以上述べてきた各情報を備えているのが管理データテーブル2であり、その論理的構成を図5に示す。

【0043】次に、計算機本体10の筐体番号の格納場所について説明する。本実施例においては筐体番号は、図6に示すように基本筐体内のSVPとCEパネル間に接続されている固有筐体アドレスボード内に格納されている。

【0044】次に、本実施例の資源利用方式におけるS/W管理について説明する。図7はS/W管理機能を実現する構成を示す概要図である。この図を用い、まずS/W管理機能の仕組みを説明する。

1) ベンダマシンからのICカード作成/変更について、図7及び図8を用いて説明する。

(1) 契約内容(S10)に従って、顧客データベースメンテナンス手段301を用い、顧客データベース303を生成/更新する(S11)。

(2) 次にS12において、ICカード作成手段302を用いて、更新された顧客データベース303からICカードの作成/変更を行う。ICカード作成手段302は、ICカードに関するSVCインタフェース306、カーネル304を用いてICカードのREAD/WRITE等を行う。

【0045】2) ユーザマシンでの動作について図7及び図9を用いて説明する。

(1) IPL時、他のイニシャライザプログラムにさきがけてICカードチェック手段307が実行され、ICカードに関して図9に示すフローに従ってチェックを行う。ICカードの内容に変更が生じた場合にはその都度チェックが必要となる。

(a) 特権フラグが設定されているか？(S20)  
特権フラグはICカード内の情報ではなくOS内部に持つ情報である。このフラグを設定することにより、ICカードのチェックなしで全てのソフトウェアを動作させることができる。なお、この機能は非公開とする。

(b) 正常なICカードが装着されているか？(S21)

ICカードへのアクセスがエラーとなる場合(ICカー

ドが装着されていない場合も含む) SVPディスク311に格納されている以前に記憶された管理データテーブルを読み込む(S23、S24)。SVPディスク311に管理データテーブルがない場合には最低限の機能を実行できる縮退モードで立ち上がる(S23、S33)。SVPディスクの情報から立ち上がる場合には、そのファイルの生成日が調べられ、一定期間以上経過していた場合には縮退モードで立ち上がる(S25、S33)。

10 (c) ICカード内の管理データテーブルの読み込み(S22)

読み込む情報には以下のようなものがある。

読み込まれる情報：ユーザレベル、動作可能CPU台数、CPUシステム番号、OS名、OS版名(バージョン名ともいう)と有効期限、使用可能なS/Wの種類・版名・有効期限・製品クラスetc.

(d) 読み込んだ管理データテーブルの正当性チェック(S26)

ADFの持つAPW(ADF毎のパスワード)と照合するために、セキュリティ管理プログラムは、ICカードを使用してシステムを立ち上げようとするユーザにパスワードの入力を要求する。そしてセキュリティ管理プログラムは、コンソールから入力されたパスワードとAPWをチェックし、異なると判定された場合には縮退モードで立ち上がる。契約期限切れの近いS/Wに関しては、IPL時メッセージでその旨を通知する(S27、S28)。

(e) 読み込んだ管理データテーブルのメモリ上のICカード情報テーブル305への格納(S29)

30 前述した(d)のチェックがOKであった場合、ICカードから読み込んだ管理データテーブルをメモリ上のICカード情報テーブル305へ格納する。ICカード情報テーブル305はメモリダンプ等で解読されないよう暗号化する。また、前述した(b)の次のIPL時チェック(S21、S23)で使うため、ICカード内の管理データテーブルをSVPディスク311へ書き込む(S30)。

(f) IPL回数の加算(S31)

40 前述した(d)で正常と判断された場合には、メモリ上のICカード情報テーブル305のIPL回数に1加算する。

【0046】(2) ICカードチェック手段307の動作により正常なシステムと判断された場合通常のIPLが実行され、以後各S/Wはその起動時以下の方法によってOSによる起動時チェックを受け、契約S/Wのみが動作する。その機能の動作時必ず実行されるモジュール(IPL時イニシャライザ等)の動作の先頭で、OSが提供するSVCインタフェース306のチェックシステムコールを呼ぶ。それがノーマルリターンした場合以外はエラー終了させる。SVCインタフェース306の

チェックシステムコールは、引数としてその製品のコード、版名等をもらい、ICカード情報テーブル306と照らし合わせ、動作可/不可、製品クラス等を返す。また、起動回数をカウントしたいS/W製品に関しては、その意志を伝える引数も渡す。これにより、IPL後シャットダウンするまでの起動回数がメモリ上に記録され、シャットダウン時、それがICカード上の管理データテーブル中の累積起動回数に加算される。

【0047】(3) ICカードの管理データテーブルをモニタする管理データテーブルモニタ機能310(図7参照)を提供し、ユーザレベルでどのソフトウェアが動作可能かを確かめできるようにする。

【0048】次にアプリケーションプログラムからのSVCインタフェース306のチェックシステムコールについて説明する。各S/Wは、メインとなるモジュールおよびn個のサブモジュールから構成されている。S/Wはメインとなるモジュールが起動された直後本システムコールを呼び出し、リターン値を受け取る。OSによるICカード情報テーブルとのチェックを行い、そのリターン値が正常値である場合のみ動作を続行し、エラーリターンした場合にはその旨をメッセージ出力し、アボートさせる。本システムコールが呼び出される箇所は、  
1) イニシャライザ、ユーザから直接呼び出せるロードモジュールの先頭等、その箇所であボートすることにより、その機能が使い物にならない箇所であること、  
2) アボートしたことをユーザが気付く易い箇所であること、  
3) コール回数が必要最小限であること。起動回数をカウントする必要があるものは、その値が意味のあるような箇所であること、  
という条件を満たさなければならない。

【0049】次に被プロテクトノードがH/Wの場合について説明する。この実施例においては、管理データテーブル内のユーザ管理情報にその計算機システムにおいてOSがサポートできるH/Wの制限数あるいは制御量に関する情報が記述されているものとする。SVPはまた、計算機の持っている日付が、ユーザ管理情報の中の使用開始可能日と有効期限の間であることを確認する。もし有効期限の間でなければ以降のチェックは行わない。システムの立ち上げ時に、サービスプロセッサはH/Wの制限数あるいは制御量に関する情報を参照する。また、サービスプロセッサは、その計算機に接続されている各H/Wの構成を独自のやりとりによって確認する機能を有している。そして、確認したH/Wの台数を記憶するレジスタを有し、そのレジスタに書き込まれた台数とユーザ管理情報内の制限数を比較し、制限数の範囲内であれば、そのH/Wを正式にこれから立ち上げる計算機のシステム構成に加えて、IPLを行う。例えば、ユーザ管理情報において制限されたワークステーション台数が3台(まで)と記述されているとき、実際に物理

的に接続されているワークステーションが2台であったとき、その2台のワークステーションは論理的にも計算機に接続が許可され、使用可能となる。また、物理的に接続されているワークステーションが3台であっても、ユーザ管理情報において記述されている台数以内、すなわち3台以内であるので、同様に接続が許可され、その計算機において使用可能となる。

【0050】次に、物理的に接続されているワークステーション台数が4台以上であった場合を説明する。この場合、最初の3台までは接続が許可されるが、4台目以降のワークステーションは物理的に線はつながっていても、計算機のシステム構成には含まれない。ここで、最初の3台というのはSVPによって認識される順序によるので、どのワークステーションが接続不可となるのかはSVPに依存している。ここではワークステーションを例にとって説明したが、台数で数えられるH/Wに関しては同様に判断される。すなわち、FXD(固定ディスク)、データベースプロセッサ、MTなどである。

【0051】次に、被プロテクトノードが主記憶装置である場合について述べる。主記憶装置がメモリーボード単位で数えられるとき、その数によって前述したように計算機での使用を制限することができる。また他の方法として、実装されている全てのメモリーに一連のアドレスがふられているときは、使用可能なアドレス範囲情報を指定することによって、その識別カードを持つユーザに許可されている容量を使用可能とするやり方でもよい。また、この2つの方式は被プロテクトノードがキャッシュメモリで、ハード的に設定されている場合にも適用可能である。つまりキャッシュメモリに割り当てるメモリーボードを枚数で制限する方法と、キャッシュメモリ用として使用するメモリーのアドレスを指定する方法である。あるいは、キャッシュメモリがソフト的に実現されている場合には、キャッシュメモリ管理用のソフトウェアを本方式のS/W管理の対象としておくことによって、使用を制限することも可能である。さらにこれらの方式を組み合わせることによって、全ての整合性がとれた場合のみ、実際にキャッシュメモリを使用可能とする方法も有効である。

【0052】次に、被プロテクトノードが計算機クロック周波数であった場合について述べる。これにはシステム立ち上げ時にパラメータを受け取ることによって、指定されたクロック周波数を発生させる手段が計算機にあらかじめ備えられていることを前提としている。計算機はSVPによって管理データテーブルからユーザに許可されたクロック周波数を受け取り、そのクロック周波数で稼働する。

【0053】以上のように、この実施例に係わるプログラムロード方式及び周辺機器インストール方式計算機は計算機筐体に設けられた個別の識別子とその計算機にオブションとして接続されるH/W、或はその計算機上で

動作するS/Wを、識別カードおよびSVPにより、カード内に記録された被プロテクトノードを記述した管理データテーブルのデータに従って認証させ、それらの接続あるいは起動を制限するものである。

【0054】本実施例においては、認証用の識別カードは当該計算機に対し一枚しか存在せず、それぞれ対応する一台の計算機においてでしか機能しないので、識別カードの対象計算機が限定されることによって、その計算機で使用されるS/Wあるいは周辺機器の制限情報は確実に固有のものとなり、セキュリティ効果は増大する。また、識別カードを使用することにより、その中へ格納する被プロテクトノードを記述した管理データテーブルのデータを不法に読取、改ざんされる危険を防止する。そしてその対象を動作するプログラムのみではなく、接続されるH/Wコンフィグレーション情報まで広げることにより、容易なモデルレパートリの拡張を実現する。またSVPに識別カードとのインタフェースを設けることにより、既存の基本処理装置、各周辺機器コントローラは変更する必要はなく、容易にシステムに組入れる事ができる。更にSVPを経由して遠隔地から識別カードのアクセスを可能にすることにより、被プロテクトノードを記述した管理データテーブルの読取、更新を遠隔地から行うことを可能にする。

【0055】この実施例の利点として、以下のようなものがあげられる。

- ・ユーザシステム側で自身のシステムの正当性を判定できる。
- ・より万全なセキュリティシステムの提供。
- ・必要な機能だけ購入できるOS分の分割化。
- ・S/Wの試使用制度等の新しいサービスの提供。(遠隔保守システムと連携した場合)
- ・SE作業の省力化。
- ・販社S/Wの不正使用防止対策を支援。
- ・S/W製品の契約による売上の確保。
- ・保守性向上。
- ・出荷作業の省力化。
- ・ロイヤリティ支払いの適正化。
- ・メーカーによる顧客管理の実施。

また、この実施例によれば、システムの不正使用の防止をはかることができる。また、顧客管理システムを導入することにより、ユーザ登録制度を実施し、メーカーでも顧客管理ができる。

【0056】以上のような手順で、ユーザシステムにおいて筐体管理情報を用いて、システムの正当性を判定する。筐体管理情報は、図6に示すようにH/W本体に出荷時から格納されているので、CPUシステム番号のようにボードの交換等で入れかわって他の内容で書き換えられてしまうということは発生しない。また、ソフトウェアから読み出し可能としたので、人手をわずらわすことなく、自動的に読み取りを行うことができる。この特

徴を活かして、ユーザシステムで動作する保守システムは、システム立ち上げ時に筐体管理情報を毎回取り込むようにしている。そして、取り込んだ筐体番号を使用してシステム立ち上げ時に正当なシステムであることを確認する。

【0057】次に、保守システムについて説明する。図10はこの実施例の保守システムの機能図である。図において、400はユーザシステム、411は管理情報記憶部、412は正当性判定部、413は情報送信部である。また、600はセンタシステム、611は情報登録部、612は照合部、613は保守部である。図11はこの実施例のハードウェア構成の一例を示す図である。図において、5は筐体管理情報、10は計算機本体である。計算機本体10はCPU、主記憶装置、通信制御装置、ディスク制御装置等から構成されている。これらのCPUや各種制御装置は不良発生時の交換ユニット単位である。従来から計算機システムの識別子としてCPUシステム番号を用いる場合があった。前述したように、CPUシステム番号はCPUボードに付与されているが、CPUボードは故障等が発生した場合、必要に応じて交換されるものである。従って、CPUシステム番号はCPUボードの交換に伴い変更されてしまう場合がある。そのため、厳密な意味ではユニークな識別子とは言えない。それに対して筐体管理情報5はH/W本体の交換以外では変更されない。また、通常の場合、H/W本体の交換はほとんど行われない。従って、H/W本体に記憶されている筐体管理情報はユニークであると言える。しかも、業務システム稼働時には必要としない情報であるので、保守システムで利用しやすい。筐体管理情報の格納場所は、前述した図8の固有筐体アドレス・ボード内である。

【0058】図12は保守システムにおけるユーザ情報の一例を示す図である。図に示すように、ユーザ名称、ユーザ住所、ユーザ電話番号、担当者名、マシン設置場所、マシン電話番号をユーザシステムの情報として記憶する。また、さらに、ユーザシステムの情報としてH/W構成情報、S/W構成情報を記憶する。これらの情報が図10に示した管理情報記憶部411に記憶される情報である。また、管理情報記憶部411には筐体管理情報も記憶されており、正当性判定部412がシステムの正当性を判定するのに用いられる。具体的な判定の方法についてはすでに述べた通りである。正当性判定部412の判定結果に基づいて、これらの情報は情報送信部413によってセンタシステムに送信される。

【0059】図13は保守システムのネットワーク構成図である。ユーザシステムは公衆回線を通じて販社の保守ホストや技術センタと接続される。販社の保守ホストは公衆回線を通じて、保守センタや技術センタと接続される。保守センタや技術センタは、通信回線を通じて保守拠点や保守中央センタと接続される。また、一顧客内

で複数のシステムを設置しているような場合には、顧客内で親局（保守ホストに相当）を持つ場合もある。図に示すようなネットワーク構成で、原則としてユーザシステムにおいて発生した障害は保守ホストへ通報され、保守ホストにおいて障害の種類が切り分けられる。あるいは、障害の種類によっては、ユーザシステム側ですでに切り分けが完了している場合があり、このような場合にはSVP（サービスプロセッサ）により通報先が自動的に選択され自動通報が行われる。また、通報の種類によってはユーザシステムから保守ホストへ通報された後、技術センタに中継される場合もある。

【0060】また、顧客管理は全てのCPU（ユーザシステム／保守ホスト／保守センタ／保守拠点）をユニークとなるように管理するノードIDにより管理される。ノードIDは各ノードにおいてシステム管理機能によるシステム定義操作において自動的に割り振られる。従って、システム定義操作では一旦上位のノードとの回線接続が必要となる。ノードIDは保守中央センタにおいて全てが管理され、順次各ノードにおいて採番される。ノードIDの採番の流れを図14に示す。ノードIDは図14ではIDと表記されている。また、本明細書においては、ユーザ識別子またはユーザIDと呼ぶ場合もある。ユーザシステムからは、システム設置時のユーザ識別子採番要求時に保守センタシステムへパスワードと筐体番号を渡し、正当な採番要求元であることを宣言する。一方、保守センタでは採番したユーザ識別子と筐体番号でユーザ情報の管理を行う。保守ホストは保守センタにID割り付けを要求する。同様に、各ノードは上位のノードに採番要求を行い、全てのノードID（ユーザ識別子）は保守中央センタにおいて管理される。保守ホストより上位のノードにおいて、下位のノードからの採番要求に従い、ユーザ情報を記憶している顧客管理ファイルのMASTERレコードを参照して採番する。図15はユーザ識別子の形式を示す図である。図に示すように、各ノードである保守センタ、保守ホスト、ユーザの番号の組み合わせで構成されているので、必ずユニークな識別子となる。ユーザ識別子の割り当て後は、システム立ち上げ時に正当なシステムであることをユーザシステム側で毎回確認する。図16はユーザシステムの立ち上げ時の処理の流れ図である。まず、計算機の電源がオンになると（S41）、S42においてIPL（インニシャルプログラムロード）が行われる。この時にネットワーク定義や接続されている周辺機器を含むハードウェア的な情報が取り込まれる。続いて、S43においてOS（オペティングシステム）が稼働する。次に、S44において各種インシャライザが開始するのと並行して、S45において遠隔保守インシャライザも起動される。次に、S46において筐体管理情報が獲得される。筐体番号はハードウェア本体の中に組み込まれているので、システムバスを通してメーカの特殊な命令を使用すること

によって読み取りが可能となる。従って、通常のアプリケーションプログラムからは読むことはできない。次に、S47において獲得された筐体管理情報と記憶されている筐体管理情報の照合を行い、結果がOKであれば、S48において筐体管理情報をセーブする。この筐体管理情報のセーブはハードウェアやソフトウェアの構成に変化があった時のみ行われる。これは、保守に必要な情報を最新のものとするためである。次に、S49において遠隔保守サポートシステムが稼働する。一方、S47の筐体管理情報照合において結果がNOであった時、S50において示すように、遠隔保守のないシステムが稼働する。次に、S51において立ち上げ完了となり、業務プログラムの稼働が開始される（S52）。S48の筐体管理情報セーブにおいて保存された最新の保守に必要な情報は、ユーザシステムが保守サービスを要求するために保守センタに接続する際に、保守センタに情報送信部によって送信される。図17はユーザシステムから保守センタに接続するプロトコルを示す図である。図17において（1）に示すようにシステムの正当性はシステム立ち上げ時にすでに照合済であるので、（2）において接続要求を保守センタに送る。続いて、（3）においてユーザ識別子とシステム構成情報も保守センタに送る。保守センタでは接続要求を受けた相手のユーザシステムはすでに照合済の正当なシステムであると見なし、ユーザ管理情報を参照してユーザ照合を行い、送られて来たシステム構成情報を用いて、情報登録部に記憶されているユーザ情報を最新情報に更新する。その後、（5）において保守サービスを開始する。図18は保守センタのファイルシステムを示す図である。図に示すように、ユーザのH/W構成情報やS/W構成情報は、顧客管理ファイルとして保守センタのファイルシステムの一部に記憶されている。この実施例の保守システムは以上のように構成されているので、保守センタ側では保守センタの管理情報と整合性を確認するだけで正当性確認を終えるので、パスワードの交換やコールバックなど接続時の余分な処理が削減されるだけでなく、ユーザシステムの更新履歴を確実に連続性を保ちながら管理することができる。

【0061】また、ユーザシステムからの接続時および保守センタからの接続時に、接続相手の確認を保守センタが採番したユーザ識別子と筐体番号で照合することから、接続相手の照合が簡素化され、コールバックなどによる照合に比べ時間と回線費用（公衆回線やパケット接続だとコールバックは2倍の費用を必要とする）が削減できる。

【0062】一般に、H/W構成の変更やシステム構成の変更を行うと、変更内容をシステムに確認させるにはIPLが必要となる。当システムではIPL時にシステム構成（H/W構成、S/W構成）情報の整合性と更新有無を確認するために、当システムが何等かの目的で保

守センタとの間で更新を行うと、保守センタのユーザシステム構成情報が更新される。これにより、保守センタは常にユーザシステムの問題解析時には最新の情報に基づき、遠隔保守を行うことができる。

【0063】また、保守センタはユーザシステムとの間で交信により得た最新の構成情報を蓄積することにより、ユーザシステムの更新履歴を管理することができる。

【0064】一般に、システムの拡張・変更はシステム本体の変更ではなく、H/Wパーツ（CPU、ディスク、周辺装置）やS/Wパーツ（アプリケーション・プログラム）の追加・変更である。従って、システム拡張に伴い変更されるパーツがユーザシステムのキーとなると、変更管理の連続性を保証するには人手によるキーの変更を余儀なくされる。そこで、筐体番号を変更管理のキーとすることにより人手によるキー変更を不要にすることにより、ユーザシステムの不偏性を容易に保証することができる。

【0065】以上のように、この実施例においては、保守対象であるユーザシステムのユニーク性を確立するために筐体番号とシステム識別子を関連付けて用いる保守システムについて説明した。これにより保守対象の問題管理を継続して行うことが可能となる。

【0066】実施例2。前述した実施例においては、ユーザ識別子の採番要求時と保守サービス実行要求時のみ、保守センタと接続する場合を説明したが、他の方法でもよい。例えば、図16に示す流れ図において遠隔保守イニシャライザが動作する時点で保守センタと接続してもよい。あるいは、IPL時にシステム構成の変化があった場合、システム構成情報が書き換えられているので、書き換えた情報を保守センタに転送して、保守センタ側のユーザ管理情報も書き換えておくという運用でもよい。この場合には、保守センタは保守サービスが要求された時にユーザ管理情報を最新情報に更新する手順が不要となるので、ユーザ照会後、ただちに保守サービスを開始できるという利点がある。

【0067】実施例3。この実施例では、障害通報に基づいて保守解析情報を収集して保守センタに転送する遠隔保守方式について述べる。図19はこの実施例の遠隔保守方式の機能図である。図において、400はユーザシステム、421は保守解析情報を収集する収集手段、422は保守解析情報の中から転送する情報を選択する選択手段、423は情報を転送する転送手段である。また、600は保守センタのセンタシステムである。

【0068】次に、動作について説明する。図20は障害が発生してから修復するまでの流れ図である。ユーザシステムにおいて障害が発生すると、S60において保守解析に必要な情報をセーブする。その後、S61において障害発生を保守センタに通報する。次に、S62において回線情報の識別を行う。その後、S63において

解析情報一覧の作成を行う。S64において解析情報の送信を行うが、この時に回線のキャパシティに合わせて送信を行い、送信した解析情報あるいは送信を行わなかった解析情報に関する解析情報格納先一覧も合わせて送信する。解析情報を受け取った保守センタ側では、S65において一次解析を行い、続いてS66においてさらに分析を行う。その結果、S67において修復方法の指示を行う。ユーザシステム側では、S68において指示された方法に基づいて修復を行う。

【0069】図21は情報の優先順位による分類の図である。通報時に添付される情報には、優先順位1の基本構成情報、優先順位2の障害解析定型情報、優先順位3の通報補足情報の3種類の分類がある。基本構成情報は優先度が高く、通報時には無条件に送信される。基本構成情報の内容はユーザ情報、S/W構成情報、H/W構成情報、システム構成情報の4つからなっている。また、障害解析定型情報も優先度が高く、これも無条件に送られる情報である。この情報は一次解析に利用するものである。H/W障害に関する情報と、S/W障害に関する情報に分れている。優先順位3の通報補足情報は優先度が低いものであり、いくつかの種類に分れて記憶されている。それぞれの情報の大きさも種類によってまちまちである。

【0070】図22は回線のキャパシティに合わせて送信を判断する材料となる回線定義情報の図である。図に示すように、回線定義情報には回線プロトコル、回線種別、回線速度、インタフェース、ID番号、回線番号等がある。図21に示した情報の優先順位による分類において最も優先度の低い通報補足情報について、情報の容量による分類を行う。

【0071】図23は情報の容量による分類に用いる計算式の一例を示す図である。図において、 $\alpha$ は回線プロトコル係数であり、回線プロトコルによって増加するデータ量を係数で与える。例えば、フリーランドとバイナリ・データはそのまま送れないので文字コードに変換して転送する。コード変換の際、データ量が膨らむことになる。また、Mは転送時間であり、公衆回線、INS-C、DDX回線交換など回線接続時間で課金される回線種別の場合に用いる。情報を送るのに必要な時間の最大値で押さえるために用いられる値であり、通常2分（基本料金）である。一方、パケット系の回線種別の場合には回線速度で割る必要はなく、単に情報量をパケット数で換算し、最大転送パケット数内で送れる情報を送信する。一般に、回線速度は9600bpsでは1秒間に9600ビット=1200バイト転送可能な回線であることを示す。従って、データ量を回線速度で割ると、データを転送するのに要する時間が算出される。また、 $\Sigma$ は総和である。最初は全データの総和で判定し、Mを超えるとデータの大きいものから排除していく。できるだけ多くの種類のデータを送ろうとするので、Mを超えない

範囲におさまるまで再計算を行う。この計算式を用いて、図 2 2 に示す回線情報を参照し、通報補足情報からどの情報を送るかを判断する。この判断には回線情報に基づく計算だけでなく、通報事象によって選択を行うことも可能である。また、転送する通報補足情報は複数指定してもかまわない。さらに、判断した結果、解析補足情報が保守センタにあるか、あるいはユーザシステム内にあるかを目録として作成し、通報時に保守センタに転送する。

【0072】図 2 4 は解析補足資料の目録である解析情報格納先一覧の一例を示す図である。図に示すように、解析補足情報の目録には、データ種別、データ量、格納先などが記憶されており、例えば、データ種別 A のデータ量は 2 KB であり、格納先はセンタとなっている。また、データ種別 B はデータ量が 1 MB であり、格納先はユーザとなっている。また、データ種別 C はデータ量が 4 KB となっており、格納先はセンタである。この目録を参照することによって、センタに対して送信済のデータはデータ種別 A とデータ種別 C であることが判断できる。このような解析補足資料の目録をユーザシステムで作成し、保守センタに送信することによって保守センタでは解析に必要な資料がどこに保存されているかを正確に把握することができる。

【0073】以上のように、この実施例では回線種別により保守センタへの転送情報を選別し、解析情報の格納先を障害通報時に伝える方式を採用した遠隔保守方式について説明した。この実施例によれば、解析情報を基本情報として補足情報に分割したので、通報時に必ず転送されてくる基本情報から保守センタでの解析作業効率が改善される。また、通報事象を細分化し、通報事象毎に解析情報を選択可能とすることにより、多種多様な障害に対する解析情報を容易に拡張することが可能となり、遠隔保守での障害解析範囲を拡大が図れる。さらに、通報時に転送する解析情報を複数指定可能とすることにより、ユーザシステムと保守センタ間で柔軟な転送判断が可能となった。また、障害通報時に、回線種別を判断材料に、回線速度・回線費用・情報の種類を考慮し回線補足資料を通報元に格納するか、通報時に転送するか判断することにより、ユーザシステムからの通報時の回線費用負担を軽減できるようになった。さらに、障害通報時間が短縮されたことにより、通報補足資料採取のためのユーザシステムにおける業務中断を短縮できるようになった。また、解析補足資料を保守センタに転送するか否かの判断結果を目録として通報時に保守センタへ転送するようにした。目録により、保守センタは解析補足資料として何が何処に存在するかを明確に判断できるようになり、必要な時必要な情報を容易に参照可能となった。

【0074】実施例 4. 前述した実施例に加えて、さらに通報補足情報を分類し、それぞれ優先順位を設けてもよい。この場合、全体的な優先順位は、情報の優先順位

による分類、通報補足情報の優先順位による分類、情報の容量による分類の順となる。このようにして決定された優先順位に従って情報は、保守センタに送信される。

また、通報補足情報に優先順位を設ける際、通報するシステムで指定する順番を優先順位とする方法でもよい。

【0075】実施例 5. この実施例では、保守センタが回線を用いてユーザシステムを保守する遠隔保守システムについて述べる。保守センタの様に多種多様な相手と接続し、多種多様なサービスを提供しなければならない場合、用途に応じて複数の回線を必要とする。また、きめ細かなサービスを提供するには 1 本の回線を多用途に利用できるようにする必要がある。この実施例では、回線を有効に利用できる回線接続について説明する。

【0076】図 2 5 はこの実施例の機能図である。図において、400 はユーザシステム、600 は保守センタである。631 はユーザシステム 400 に対して接続要求を出す接続要求手段、632 はユーザシステムからの接続応答に対して折り返し接続要求を出す折り返し接続要求手段、633 は回線の接続を切断する回線切断手段である。また、431 は保守センタ 600 の接続要求手段 631 に基づく接続要求に対して応答する応答手段、432 は折り返し接続要求手段 632 に基づく折り返し接続要求に対して接続要求を出す折り返し手段である。

【0077】次に、動作について図を用いて説明する。

図 2 6 は折り返し接続の手順を示す流れ図である。保守センタは保守解析を開始すると (S70)、S70 において接続要求をユーザシステムに対して送り出す。ユーザシステムは保守センタからの接続要求を受けると、S72 においてセンタ連携プログラムを起動する。続いて、S73 において接続応答を保守センタに対して送る。保守センタでは、S74 において折り返し接続要求を出し、S75 において回線切断を行い、回線接続待ち状態となる (S76)。ユーザシステムでは、保守センタからの折り返し接続要求に答えて、一旦回線切断した後 (S77)、S78 において接続要求を出す。保守センタは、その接続要求に対して、S79 において接続応答を出す。その後、S80 において作業を開始する。一般に回線費用は発呼側か着呼側に一方的に決定されてしまう。このような折り返し接続の接続を可能にすることによって、保守センタから監視する保守解析作業においても、実際の保守作業開始の直前にユーザシステムから接続要求を出されることによって、ユーザシステム側に回線費用を負担させることができる。次に、図を用いてこの折り返し接続のために追加されるインタフェースを具体的に示す。図 2 7 は通常の接続処理における発呼側と着呼側の手順である。また、図 2 8 は着呼側制御プロが着呼側サブプログラムを起動し、機能情報、発呼側から機能情報に対応した処理を行う手順を示す図である。図 2 9 はこの実施例の折り返し接続処理を行う場合の手順の図である。枠で囲まれた部分のインタフェースが図



27に示した通常の接続手順、通常の接続処理に追加されている。

【0078】次に、保守センタのオペレーションが中断する要因が発生した場合に、その中断に対応して回線を切断、あるいは回線を再接続することが可能となる一次切断について説明する。図30はこの実施例の遠隔保守システムのブロック図である。図において600は保守センタであり、641は回線を接続してユーザシステムに対して作業指示を出す指示手段であり、642は指示手段による作業指示の作業時間を判定する判定手段であり、643は判定手段642の判定結果に基づいて回線の接続を切断する回線切断手段である。また、400はユーザシステムであり、441は指示手段641による指示を実行する実行手段、442は実行手段441による実行終了後、回線の接続状態をチェックする回線状態判定手段、443は回線状態判定手段442の判定結果に基づいて回線を接続する回線接続手段である。図31は一次切断を行う場合の処理手順を示す流れ図である。保守センタは、S85において保守解析を開始し、S86において分析指示をユーザシステムに対して出す。次に、S87において判定手段がS86で出した分析指示の作業時間を判定し、長時間であれば、S88において分析中回線切断指示を出す。その後ユーザシステムは、S89において回線切断を行う。保守センタは回線切断を受けて回線接続待ち状態となる(S90)。この間にユーザシステムにおいては、S91において分析指示が実行手段によって実行され、分析結果の収集が行われる(S92)。実行終了後、S93において回線状態を回線状態判定手段が判定し、切断状態であれば、S94において回線接続手段が回線接続要求を出す。その回線接続要求に対して、保守センタが接続応答を返すと(S95)、ユーザシステムでは、S96において分析結果を送信する。その分析結果を用いて保守センタでは分析を行う(S97)。また、S87の分析作業時間判定において、短時間であると判定された場合には、回線切断指示は出されないで回線は接続したままであり、ユーザシステムにおいて回線状態判定を行った結果、接続中となり、回線接続要求を出すことなく、S96において分析結果の送信が行われる。

【0079】また、折り返し接続あるいは一次切断どちらの場合においても保守センタからの回線接続中(回線接続中)という文字をオペレータに対して表示させることによって費用負担が発生していることを示し、効率良いオペレーションを促すことができる。あるいは、文字でなく回線接続中であることを示すマークを定義し、そのマークを表示させてもよい。また、これらの表示は、例えば、点滅、あるいは色変えなどという特殊表示を行ってより注意を促す方式を取ってもよい。あるいは、単なる回線接続表示ではなく、発呼接続中、着呼接続中という表示パターンを設けてもよい。さらに、これらに付

加して課金中であるという表示を付け加えても構わない。

【0080】以上のように、この実施例では、保守センタからユーザシステムの遠隔保守を行うための回線接続において、一旦保守センタから接続後、ユーザシステムから折り返し接続することを可能とすることにより、回線費用負担を必要に応じてユーザに負担させることも可能な遠隔保守システムについて説明した。この実施例によれば、折り返し接続を行うことにより、NTT回線契約の形態に影響されることなく、保守センタにおける遠隔保守のための回線費用負担を保守センタやユーザシステム双方に負担させることが可能となった。また、一時切断を可能としたことにより、保守センタのオペレーション中に発生する「思考時間」、「割り込み」などオペレーションが中断する要因が発生した場合、容易に回線切断/回線接続が可能となり、回線接続時間で課金されるタイプの回線を使用する場合の費用負担軽減が可能となった。また、保守センタからの回線接続中、回線接続状態を文字やマークで表示するのでオペレータは費用負担が発生しているのか否かが一目瞭然となり、効率良いオペレーションを心がけることができるようになった。

【0081】

【発明の効果】この発明によれば、ユーザシステムとセンタシステムの接続時に、接続相手の照合が簡素化され、時間と回線費用が削減できる。

【0082】また、この発明によれば、筐体管理情報を記憶するので、ユーザシステム情報のキー変更が不要となり、情報の連続性が保証される。

【0083】さらに、この発明によれば、保守部は記憶されたシステム構成情報を参照してユーザシステムの保守を実行するので、常に最新の情報に基づいて保守を行うことができる。

【0084】また、この発明によれば、保守に必要な情報を選択して保守センタに転送できる効果がある。

【0085】また、回線の種別に応じて補足情報を選択するので、通報時の回線費用負担を軽減できる。また、通報時間の短縮により、ユーザシステムの業務中断も短縮できる。

【0086】また、この発明によれば、補足情報の目録を保守センタに転送するので、保守センタは目録を必要な時に参照できる。

【0087】また、目録には各補足情報の存在場所を示す情報を有していることから、目録を参照して必要な時に必要な情報を容易に参照できる効果がある。

【0088】また、この発明によれば、遠隔保守のための回線費用を保守センタやユーザシステム双方に負担させることが可能となる。

【0089】また、この発明によれば、作業時間を判定し、判定結果に基づいて、回線切断/回線接続が可能となるので、接続時間に対応して課金されるタイプの回線

の費用負担を軽減できる。

【0090】さらに、この発明によれば、費用負担を意識した効率良いオペレーションを促進できる。

【図面の簡単な説明】

【図 1】 この発明の実施例 1 を示すブロック図である。

【図 2】 この発明におけるシステム立ち上げ時チェックの流れ図である。

【図 3】 この発明におけるアプリケーションプログラムの起動時の流れ図である。

【図 4】 この発明における IC カードのメモリ構造を示す図である。

【図 5】 この発明における管理データテーブルの構成を示すブロック図である。

【図 6】 この発明のソフトウェア管理機構のハードウェア構成図である。

【図 7】 この発明のソフトウェア管理機能概要図である。

【図 8】 この発明における IC カード作成までの手順を示す流れ図である。

【図 9】 この発明における IC カードチェック手段の手順を示す流れ図である。

【図 10】 この発明の保守システムの機能図である。

【図 11】 この発明の実施例のハードウェア構成の一例を示す図である。

【図 12】 この発明の保守システムにおけるユーザ情報の一例を示す図である。

【図 13】 この発明の保守システムのネットワーク構成を示す図である。

【図 14】 この発明の保守システムのユーザ識別子の採番の流れを示す図である。

【図 15】 この発明のユーザ識別子の形式を示す図である。

【図 16】 この発明のユーザシステムの立ち上げ時の処理の流れ図である。

【図 17】 ユーザシステムから保守センタに接続するプロトコルを示す図である。

【図 18】 この発明の保守センタにおけるファイルシステムの図である。

【図 19】 この発明の遠隔保守方式の機能図である。

【図 20】 この発明の障害発生から修復までの流れ図である。

【図 21】 情報の優先順位による分類を示す図である。

【図 22】 この発明の回線定義情報の図である。

【図 23】 情報の容量による分類に用いる計算式を示す図である。

【図 24】 この発明の解析補足資料の目録である解析情報格納先一覧の一例を示す図である。

【図 25】 この発明の遠隔保守システムの機能図であ

る。

【図 26】 この発明の折り返し接続の手順の流れ図である。

【図 27】 通常の接続処理を示す図である。

【図 28】 接続処理後の着呼側サブプログラム起動を示す図である。

【図 29】 この発明の折り返し接続において追加されるインタフェースを示す図である。

【図 30】 この発明の遠隔保守システムの機能図である。

【図 31】 この発明の一次切断の手順を示す流れ図である。

【図 32】 従来のユーザシステム照合方式の図である。

【図 33】 従来の保守システムの手順を示す流れ図である。

【図 34】 従来の遠隔保守の一例を示すブロック図である。

【図 35】 従来のファクシミリリモートサービスを示すブロック図である。

【図 36】 従来の遠隔保守の一例を示すブロック図である。

【図 37】 従来の遠隔保守の一例を示すブロック図である。

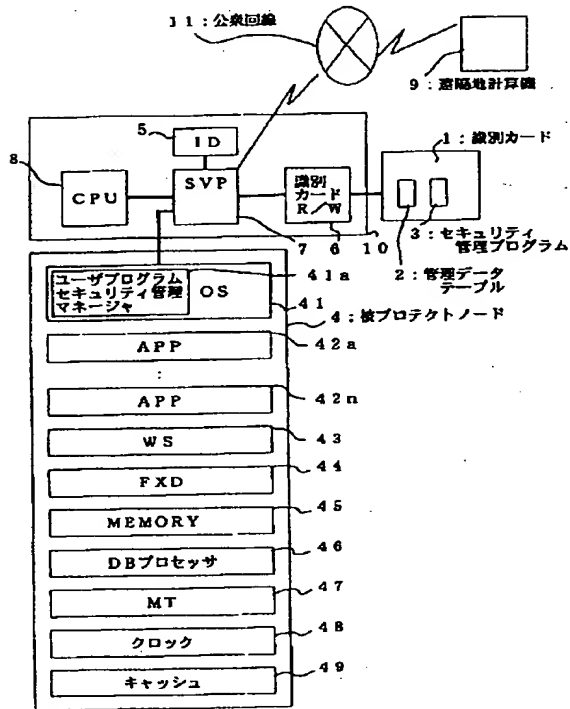
【符号の説明】

1 識別カード、2 管理データテーブル、3 セキュリティ管理プログラム、4 被プロテクトノード、5 計算機筐体に設けられた個別の識別番号、6 識別カードリーダー/ライター、7 SVP、8 中央処理装置、9 遠隔地計算機、10 計算機本体、11 公衆回線、12 識別カード、14 セキュリティ管理プログラム、17 識別カードリーダー/ライター、23 インタフェース専用 H/W、24 8ビットデータバス、25 1ビット制御線、400 ユーザシステム、411 管理情報記憶部、412 正当性判定部、413 情報送信部、421 収集手段、422 選択手段、423 転送手段、431 応答手段、432 折り返し手段、441 実行手段、442 回線状態判定手段、443 回線接続手段、600 センタシステム、611 情報登録部、612 照合部、613 保守部、631 接続要求手段、632 折り返し接続要求手段、633 回線切断手段、641 指示手段、642 判定手段、643 回線切断手段、901 情報処理システム、902 サービスプロセッサ (SVP)、903 機種タイプ保持手段、904、905 通信制御手段、906 遠隔保守センタ、907 通信回線、911 ファクシミリ装置、912 CPU、913 ROM、914 RAM、915 操作部、916 スキャナ、917 プロッタ、918 DTMF レシーバ、919 NC U、920 モデム、921 バス、924 診断装



置、931 ログ収集手段、932 自動通報判定手段、936 磁気ディスク装置、941 センタ呼出し手段、942 通報送出手段、953 フロッピーディスク、954 コンソール、955 保守試験制御部、

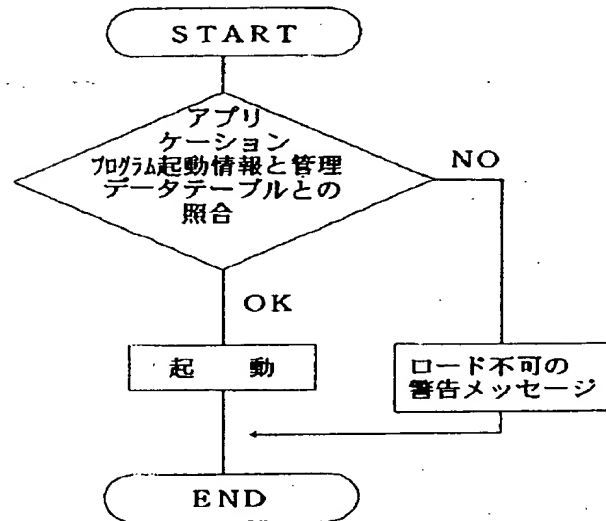
【図1】



956 操作制御部、957 転送制御部、961, 962, ... 969 周辺装置、971, 972, ... 979 障害検出手段。

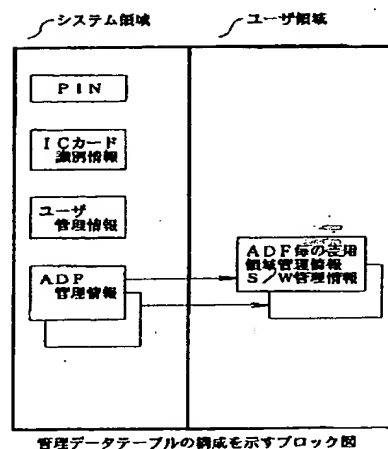
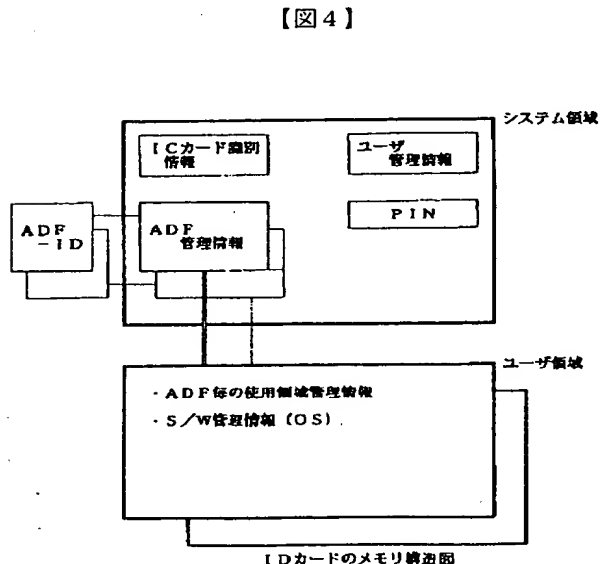
【図3】

### アプリケーションプログラムの起動



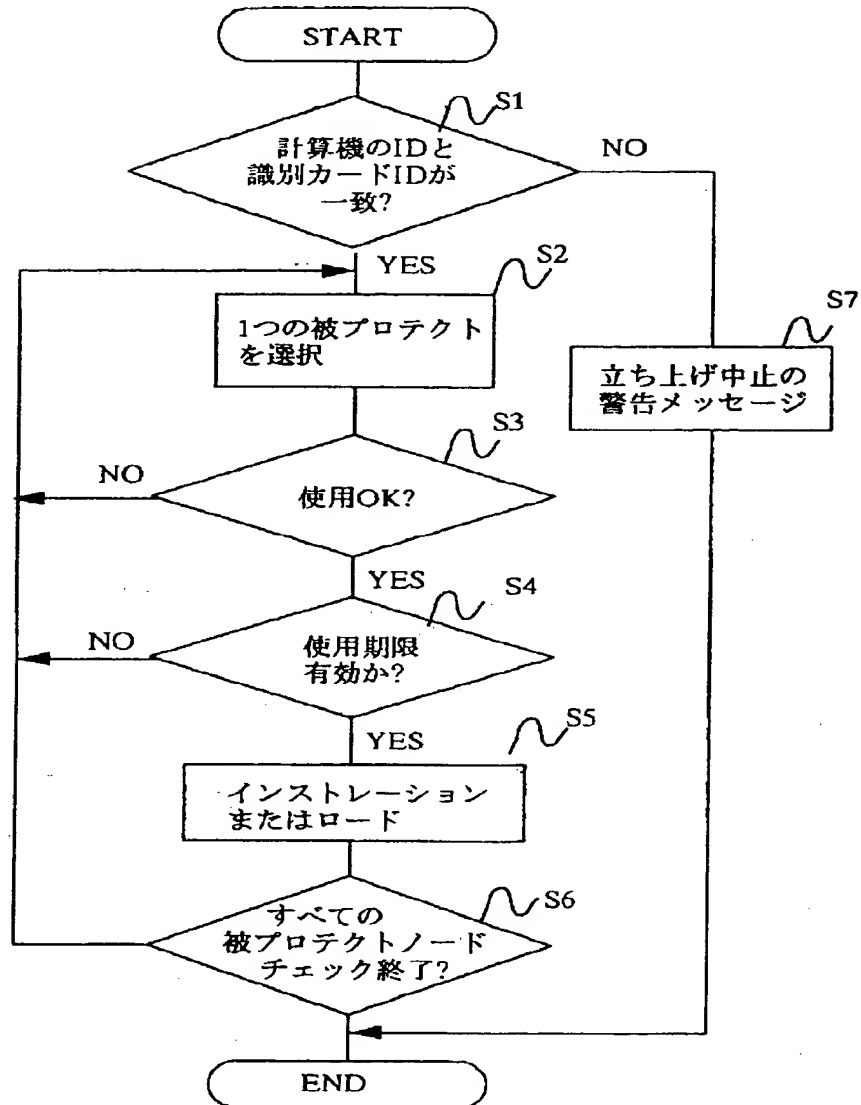
【図5】

【図4】

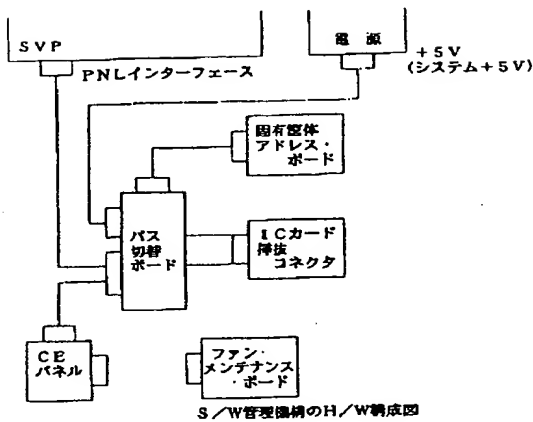


【図2】

システム立ち上げ時チェックの流れ

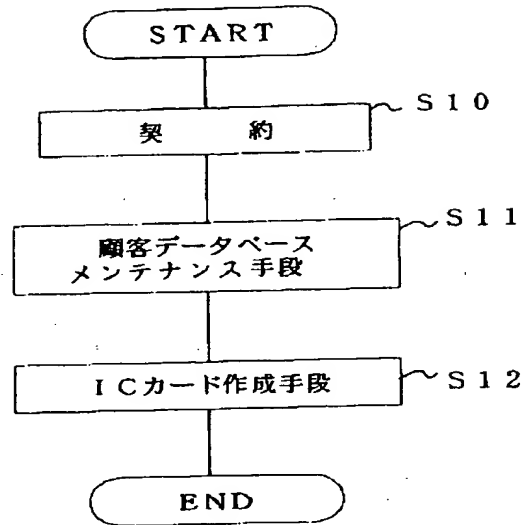


【図6】

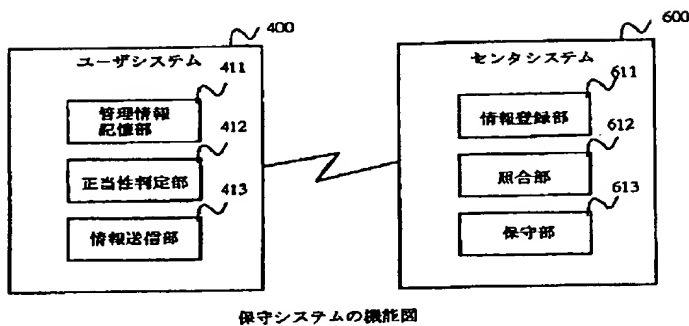


【図8】

ICカードの作成までの手順



【図10】

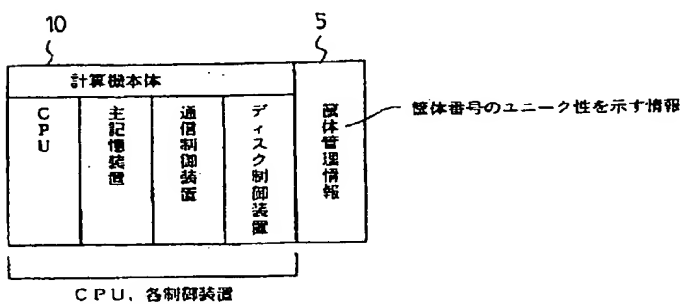


【図12】

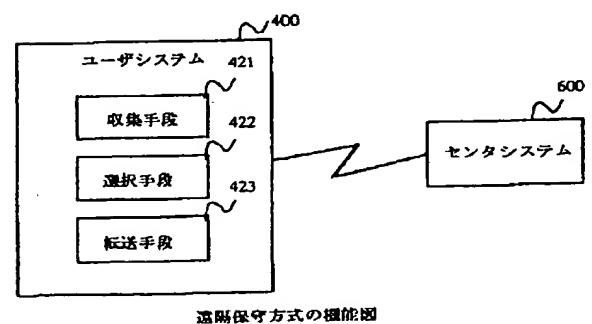
名 称	説 明
ユーザ名称	ユーザの会社名・事業所名
ユーザ住所	ユーザの住所
ユーザ電話番号	ユーザの電話番号
担当者名	ユーザの担当署名
マシン設置場所	H/Wの設置場所の住所
マシン電話番号	CPU/SVPに接続する電話番号

保守システムにおけるユーザ情報の一例

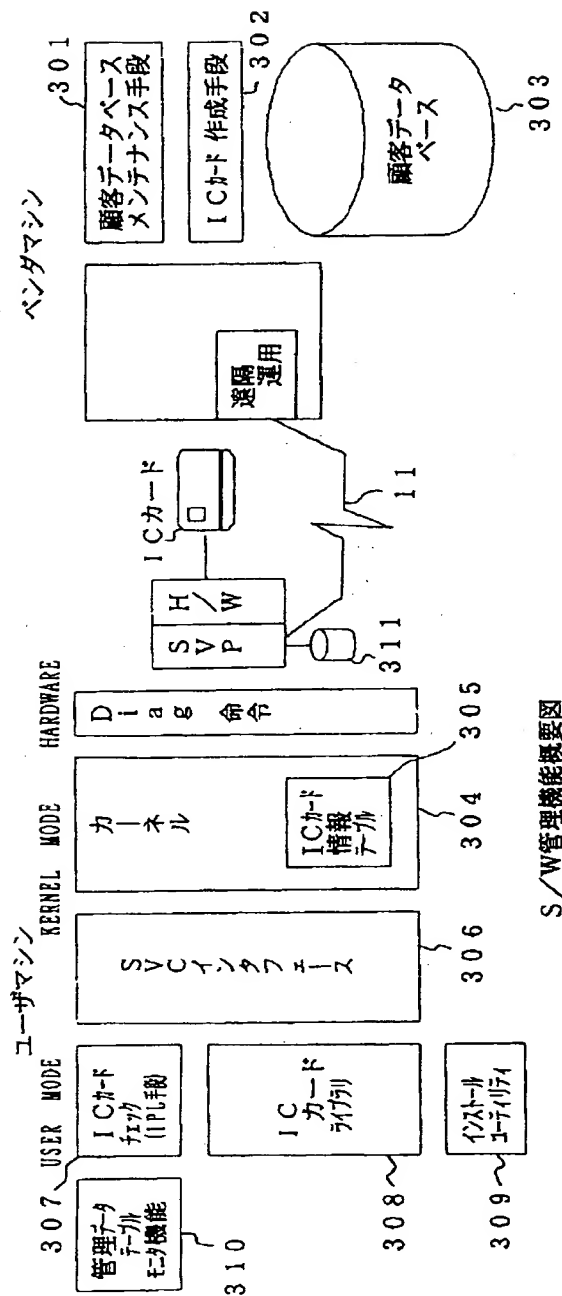
【図11】



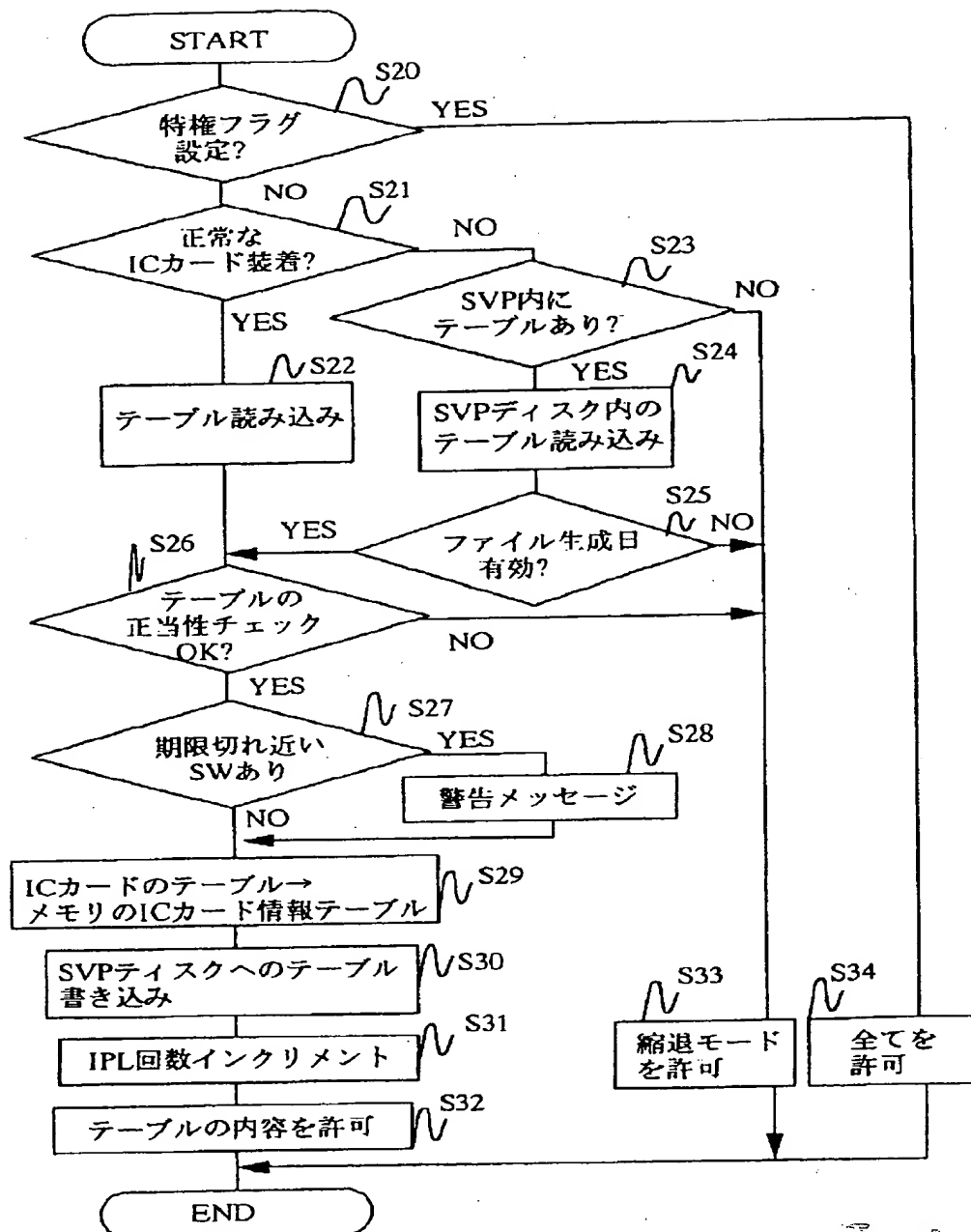
【図19】



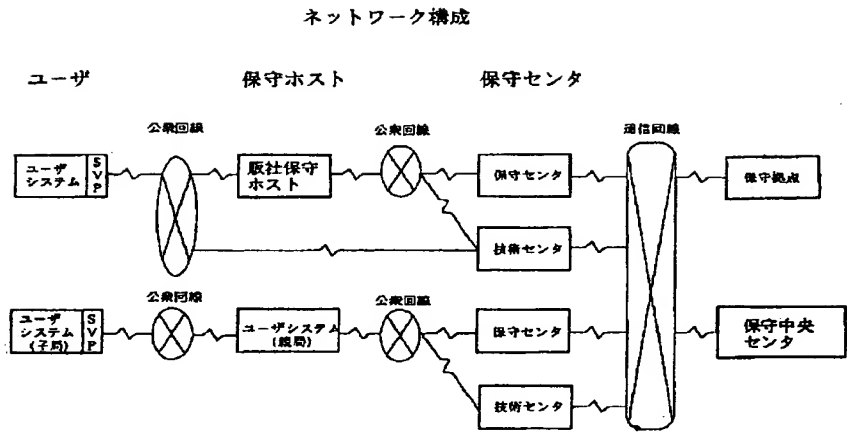
【図7】



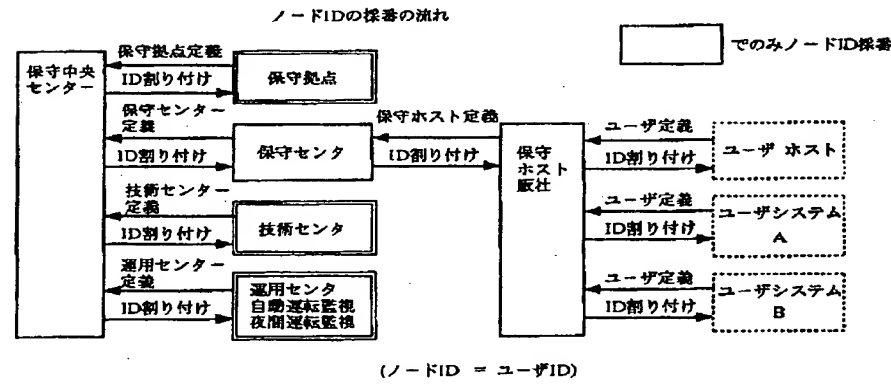
【図9】



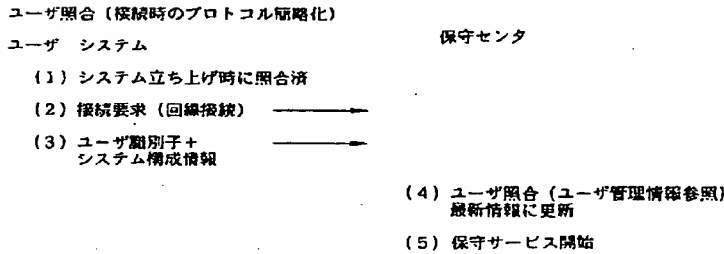
【図13】



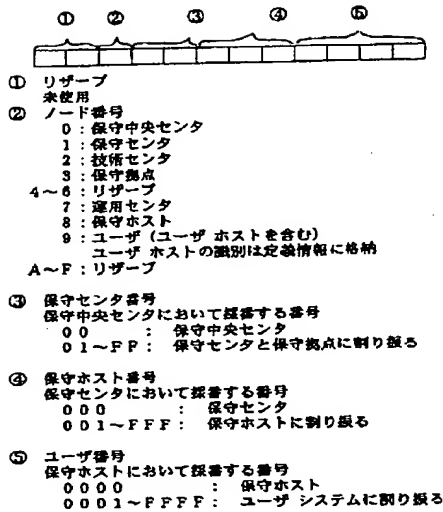
【図14】



【図17】



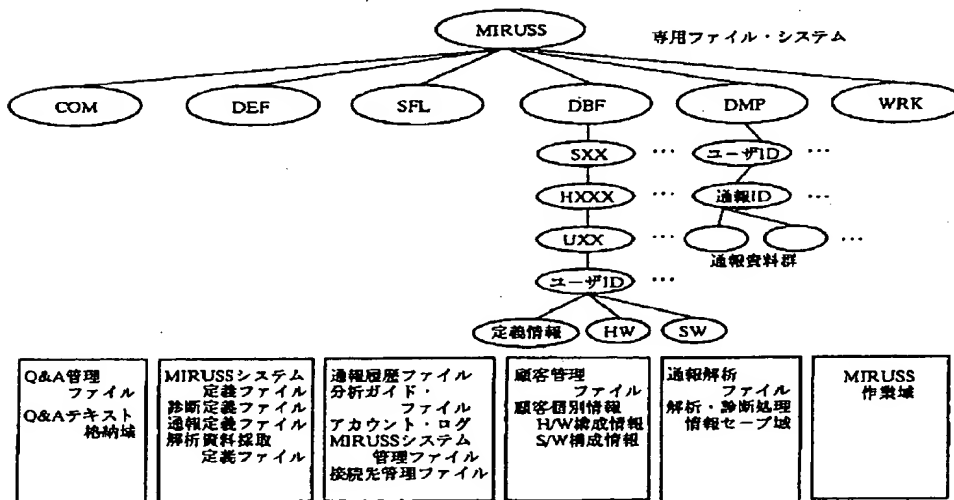
【図15】



【図21】

情報の優先順位による分類			
優先 順位	分類	内容	優先度
1	基本構成情報	ユーザ情報	高 い
		S/W 構成情報	
		H/W 構成情報	
		システム構成情報	
2	障害解析定型情報	S/W 障害	高 い
		H/W 障害	
3	通報補足情報	障害の検知場所によって 種類、量が異なる	低 い

【図18】



【図23】

$$\sum_{n=1}^{15} \frac{\text{各情報の容量 (バイト単位)} \times \alpha}{\text{回線速度}} \leq M$$

$\alpha$  : 回線プロトコル係数

$\Sigma$  : 総和

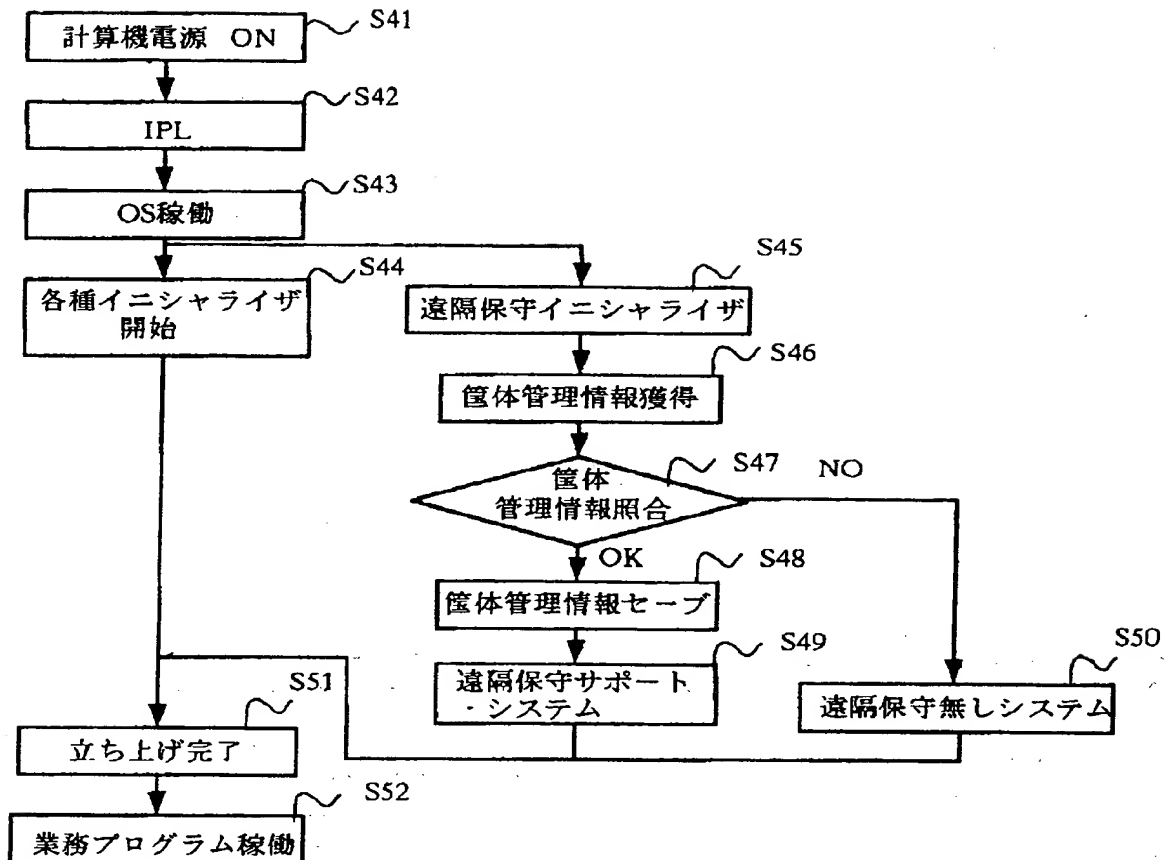
$M$  : 転送時間

【図24】

解析情報格納先一覧

	データ種別	データ量	格納先
1	A	2 KB	センサ
2	B	1 MB	ユーザ
3	C	4 KB	センサ
4		-	-
5		-	-
6		-	-

【図16】



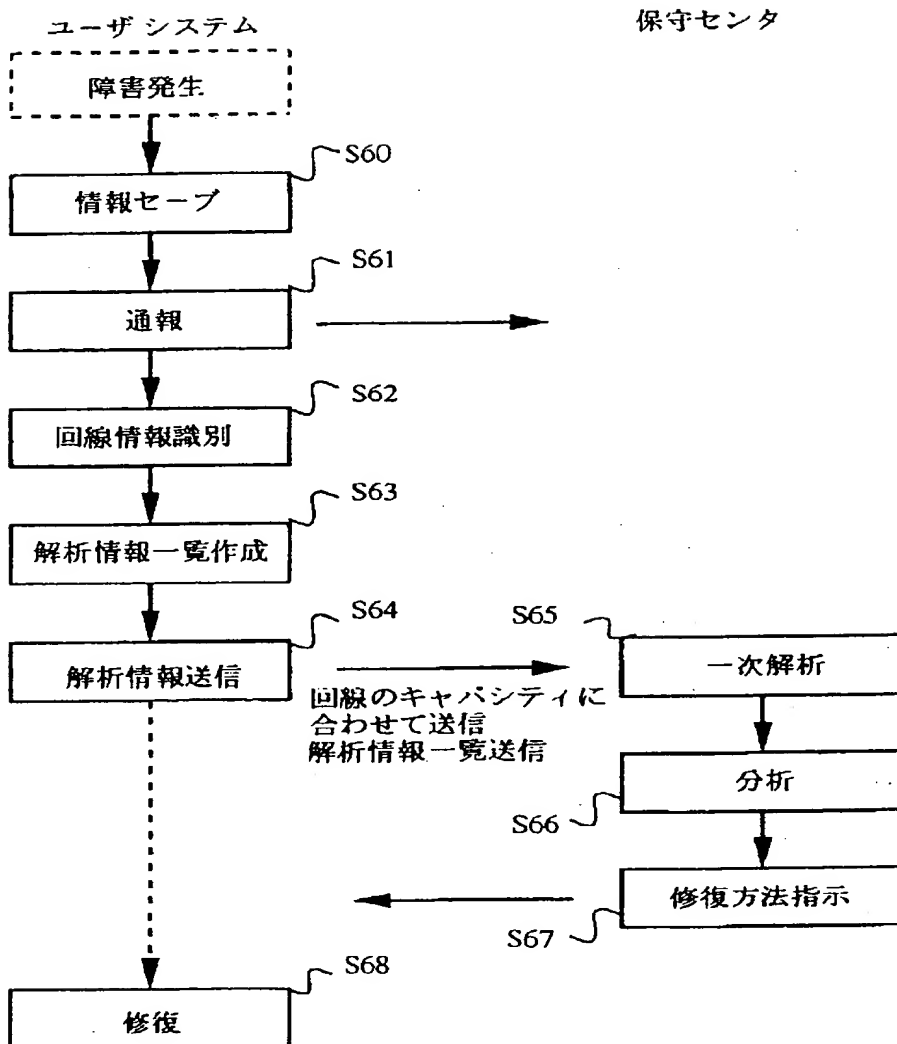
【図22】

## 図 22 接続情報

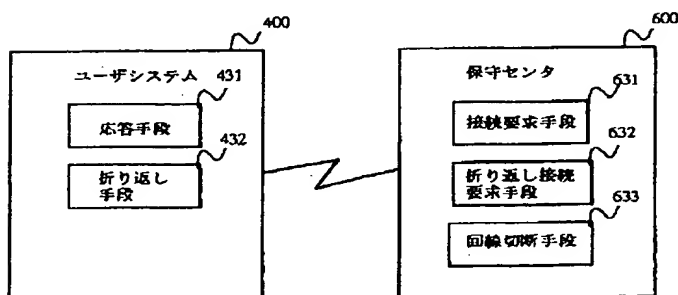
PROT...回線プロトコル フリーラン:0/BSC-C:1/BSC-P:2/X.25:3 (省略時0)  
 TYPE...回線種別 公衆回線:0/DDXパケット (又はINS-P):1/DDX回線交換 (又はINS-C):2/特定回線:3 (省略時0)  
 SPED...回線速度 1200 BPS:0/2400 BPS:1/4800 BPS:2/9600 BPS:3/19200:4/38400:5/48k:6/56k:7/64k:8 (省略時1)  
 INTF...インタフェース Xインタフェース:0/Vインタフェース:1 (省略時スペース)  
 FORM...接続形態 VC接続:0/PVC接続:1 (省略時スペース)  
 IDNO...ID番号 半角文字6字以内 (省略時スペース)  
 LINE...回線番号 半角文字20字以内 (省略不可)



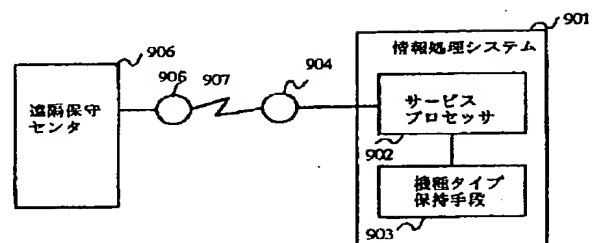
【図 20】



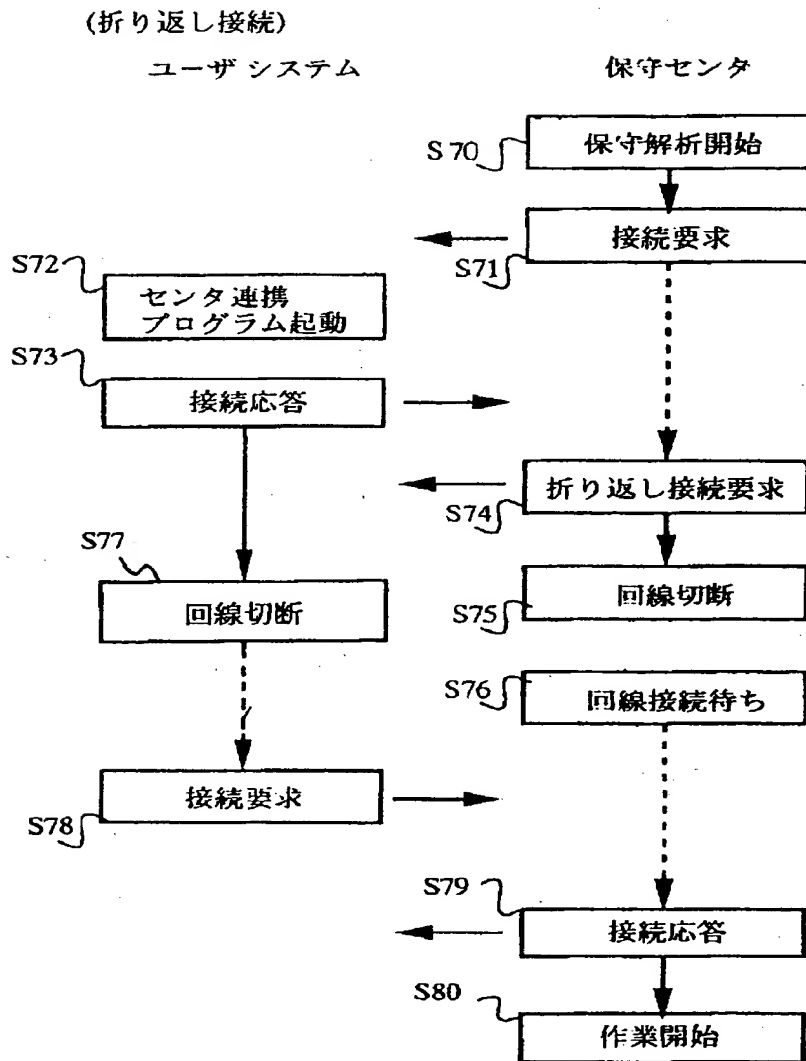
【図 25】



【図 34】



【図26】



【図27】

【通常の接続処理】

【発呼側】

発呼側プログラム起動

\_nllwp ダイアリング

SRJxxxデータ

発呼側制御情報 (00)

\_nllwt 機能情報 (01)

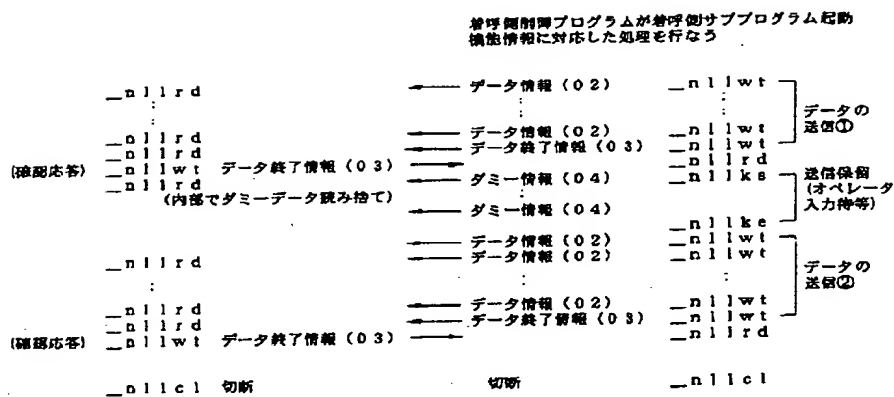
【着呼側】

着呼側制御プログラム起動

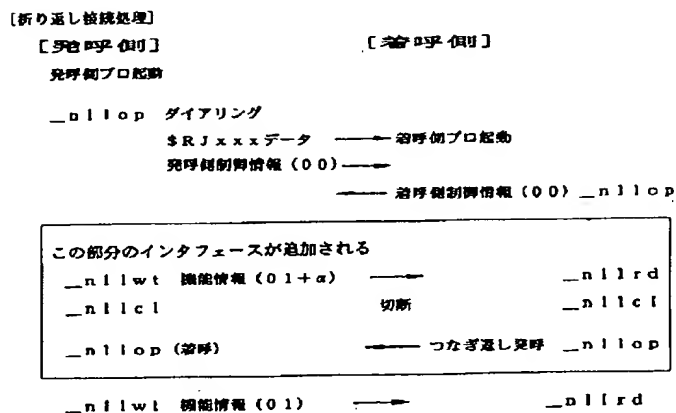
着呼側制御情報 (00) \_nllwp

\_nllrd

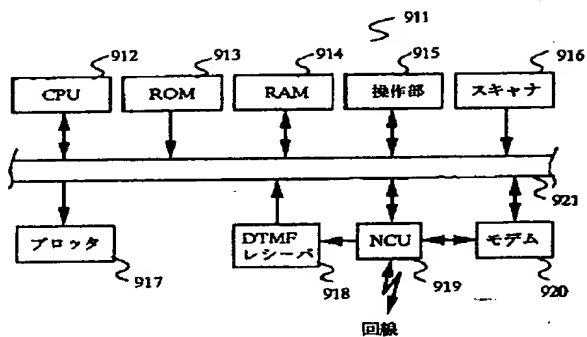
【图 28】



【图 29】

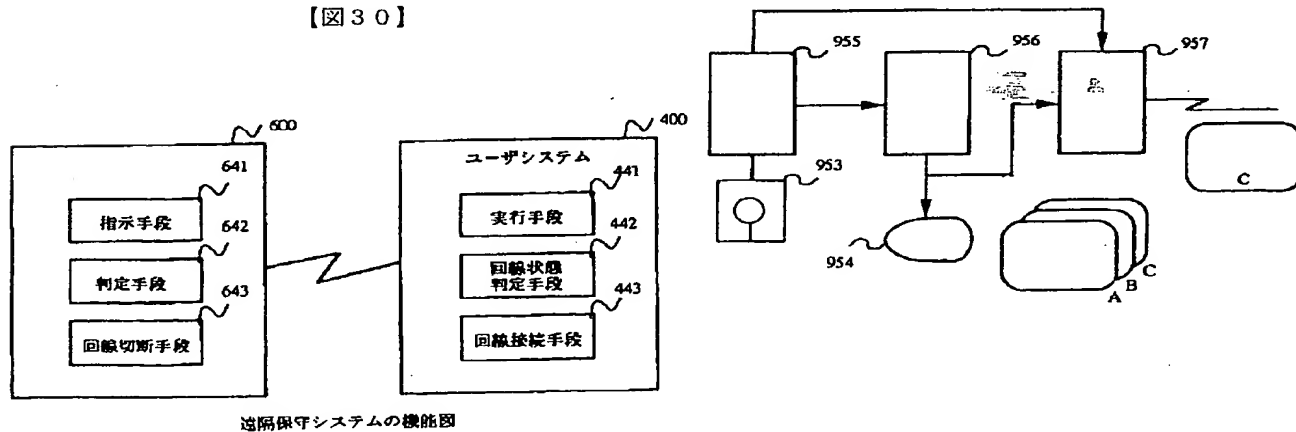


【図 3 5】



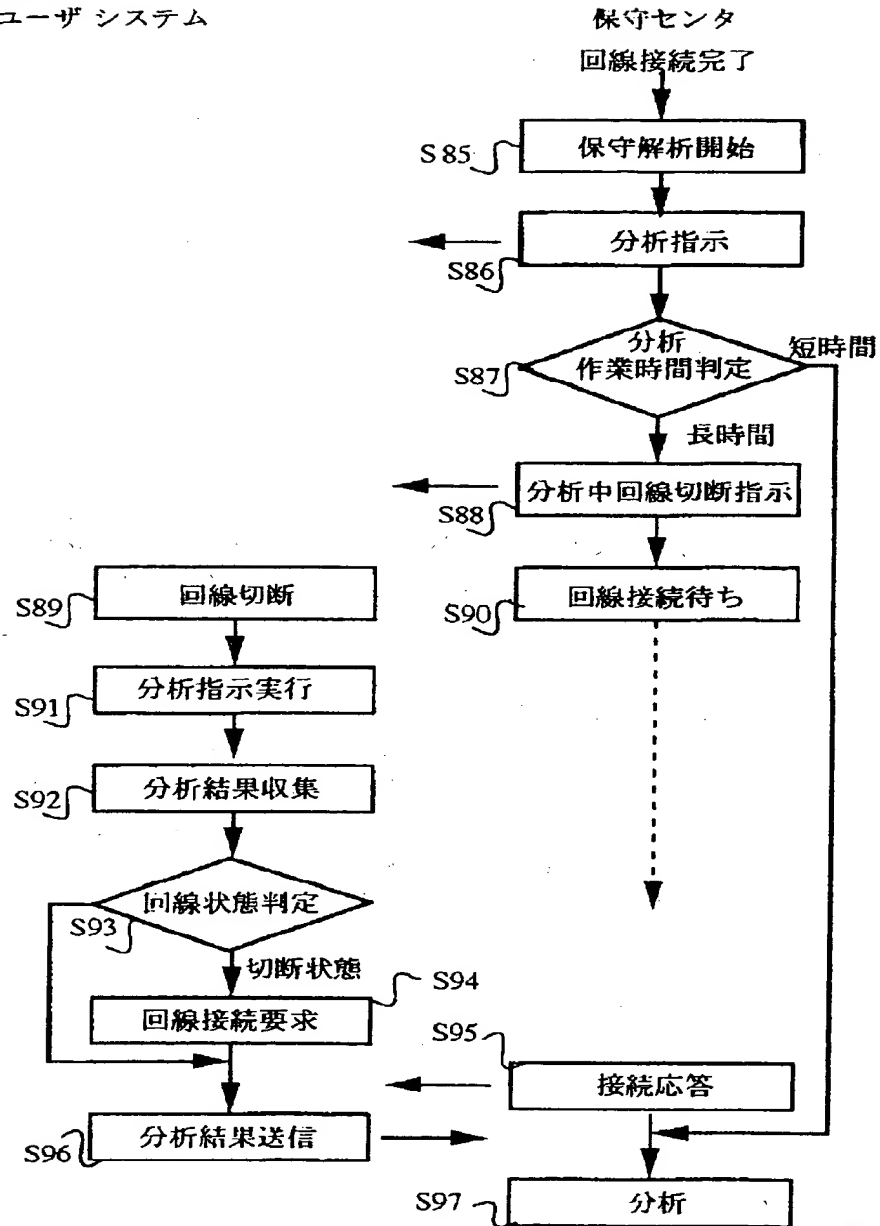
【図 3 7】

【図 30】

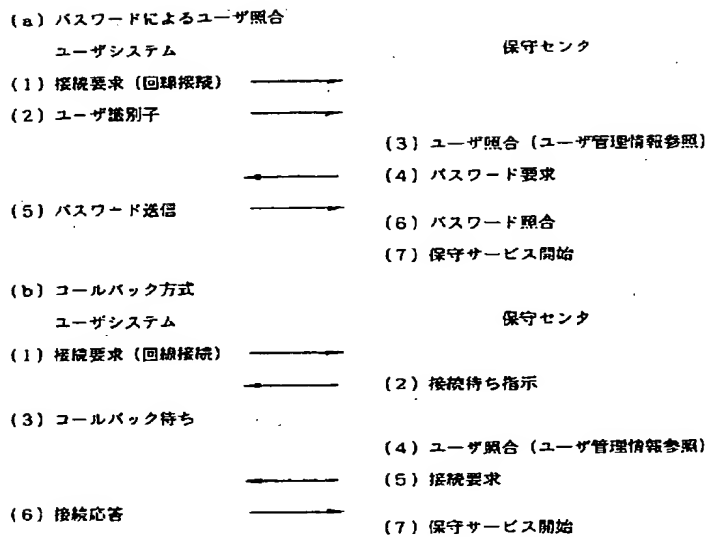


【図31】

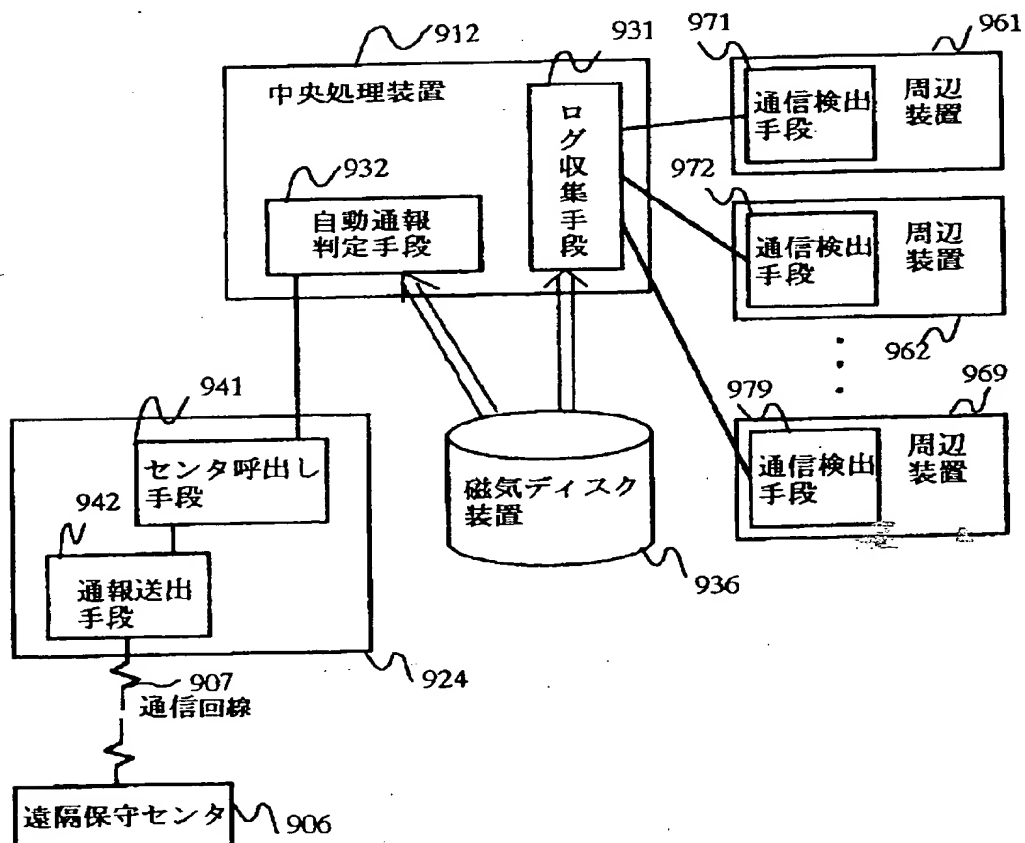
一次切断  
ユーザ システム



【図32】



【図36】



【図33】

